

LevelOne

Bedienungsanleitung

WBR-6022

HomeGuard 22 Residential Gateway

-German - Ver. 1.41

Sicherheit

FCC-WARNUNG

Dieses Gerät kann Hochfrequenzenergie erzeugen oder verwenden. Änderungen oder Modifizierungen an diesem Gerät können schädliche Interferenzen verursachen, außer die Modifizierungen sind laut Anleitung ausdrücklich gestattet. Der Benutzer könnte nicht mehr befugt sein, dieses Gerät in Betrieb zu setzen, wenn eine ungenehmigte Änderung oder Modifizierung vorgenommen wird.

Dieses Gerät wurde getestet, wobei festgestellt wurde, dass es mit den Beschränkungen für ein Digitalgerät der Klasse B, gemäß Abschnitt der 15 der FCC-Vorschriften, übereinstimmt. Diese Beschränkungen sind so ausgelegt, dass sie einen angemessenen Schutz gegen schädliche Interferenzen bei Installation in einer Wohnumgebung bieten. Dieses Gerät erzeugt und verwendet Hochfrequenzenergie, kann diese auch erzeugen, und kann den Funkverkehr empfindlich stören, wenn es nicht anweisungsgemäß installiert wurde. Es gibt jedoch keine Garantie, dass bei einer bestimmten Installation keine Interferenzen auftreten werden. Wenn dieses Gerät den Radio- oder Fernsehempfang tatsächlich stark stören sollte, was sich durch Aus- und Einschalten des Geräts feststellen lässt, ist der Benutzer angehalten, diese Störung anhand einer oder mehrerer Maßnahmen wie folgt zu beheben:

1) Richten Sie die Empfangsantenne neu aus oder versetzen Sie sie.
2) Vergrößern Sie den Abstand zwischen Gerät und Empfänger.
3) Schließen Sie das Gerät an eine Steckdose an, die mit dem Stromkreis des angeschlossenen Empfängers nicht in Verbindung steht.
4) Bitten Sie den Händler oder einen erfahrenen Radio/Fernsehtechniker um Unterstützung.

CE-Konformitätserklärung

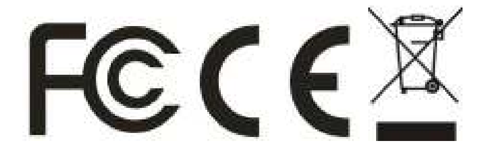
Dieses Gerät ist in Übereinstimmung mit den Anforderungen hinsichtlich elektromagnetischer Verträglichkeit, EN 55022 Klasse B für ITE, die wesentliche Schutzanforderung der Europaratsrichtlinie 89/336/EWG hinsichtlich der Angleichung von Gesetzen der Mitgliedsstaaten in Bezug auf elektromagnetischer Verträglichkeit.

CE-Warnkennzeichnung

Hiermit erklärt Digital Data Communications, dass dieses Produkt (Modellnr. WBR-6022) in Übereinstimmung mit den wesentlichen Anforderungen und weiteren dazugehörigen Bestimmungen der Richtlinie 1999/5/EG ist.

Die CE-Konformitätserklärung ist für einen Download verfügbar unter:

http://www.levelone.eu/support.php



General Public License (Allgemein öffentliche Lizenz)

Dieses Produkt bedient sich des Open Source-Codes in der Software und fällt daher unter die Richtlinien, die vom GPL-Vertrag (General Public License, Allgemein öffentliche Lizenz) bestimmt werden.

In Übereinstimmung mit den GPL-Anforderungen steht der Open Source-Code und die Open Source-Lizenz für den Open Source-Code für einen freien Download unter http://global.level1.com zur Verfügung.

Wenn Sie eine Kopie des GPL-Vertrags oder anderen Open Source-Code in dieser Software auf einem CD-Träger erhalten möchten, bietet Ihnen LevelOne (Digital Data Communications) an, diese CD auf Anfrage zu einem Preis von US-Dollar 9,99 plus Versandkosten zuzusenden.

Inhaltsverzeichnis

Standardeinstellungen

IP-Adresse	192.168.0.1
Benutzername	admin
Kennwort	password
Drahtlosmodus	Enable (Aktivieren)
Drahtlos-SSID	LevelOne
Drahtlossicherheit	None (Nichts)

1 Einführung

Glückwunsch zum Kauf des WBR-6022 *HomeGuard 22 Residential Gateways* von LevelOne. Dieses Produkt ist speziell für den Bedarf von Klein- und Heimbüros (SOHO) entwickelt worden. Es bietet eine umfassende SOHO-Lösung für das Surfen im Internet und ist einfach zu konfigurieren und zu bedienen, auch für Benutzer ohne technischen Hintergrund.

Diese Anleitung enthält Anweisungen für die Installation und Konfiguration dieses Produkts. Bevor Sie dieses Produkt installieren und in Betrieb setzen, lesen Sie bitte erst die Bedienungsanleitung, um alle Funktionen dieses Produkts nutzen zu können.

Übersicht über die Bedienungsanleitung

Einführung	Beschreibt den *HomeGuard 22 Residential Gateway*.
Auspacken und Einrichtung	Hilft Benutzern bei der grundlegenden Installation des Routers.
Hardware-Installation	Beschreibt die LED-Anzeigen des Routers.
Konfiguration	Erklärt den Funktionsumfang und die betreffenden Einstellungen.
Technische Daten	Listet die technischen Daten (allgemein und bezogen auf das Gerät und die Umgebung) des Routers auf.

2 Auspacken und Einrichtung

Dieses Kapitel beschreibt den Inhalt des Produktkartons und informiert über die Einrichtung des *HomeGuard 22 Residential Gateways*.

Merkmale

HomeGuard-Funktionen

- **Kameraansicht**
  Wenn Sie unterstützende IP-Kameras mit diesem Gerät koppeln, kann der Bildschirm der Kamera auf der Weboberfläche angezeigt werden.
- **Kameraaufnahme**
  Wenn Sie unterstützende IP-Kameras und Speichergeräte mit diesem Gerät koppeln, können Videodaten von der Kamera auf der Festplatte gespeichert werden. Es werden sowohl programmierte als auch manuelle Aufnahmen unterstützt.
- **Level1DNS.net**
  Im WBR-6022 ist ein DDNS-Konto für einen problemlosen ferngesteuerten Zugang zum Internet integriert; das Standard-DDNS-Konto kann von Benutzern auch mit Level1DNS.com (Level1-Dienst) modifiziert werden.

Grundfunktionen des Routers

- **Ethernet-Switch mit automatischer Abtastfunktion**
  Ausgestattet mit einem 4-Port-Ethernet-Switch mit automatischer Abtastfunktion.
- **Unterstützter WAN-Typ**
  Der Router unterstützt einige WAN-Typen, Statisch, Dynamisch, PPPoE , PPTP ,L2TP, Dynamisches IP mit Road Runner.
- **Firewall**
  Alle unerwünschten Pakete von externen Eindringlingen werden zum Schutz Ihres Intranets blockiert.
- **Unterstützter DHCP-Server**
  Alle vernetzten Computer können TCP/IP-Einstellungen von diesem Produkt automatisch beziehen.
- **Webbasierte Konfiguration**
  Kann über Webbrowser auf vernetzten Computern mit Netscape oder Internet Explorer konfiguriert werden.
- **Unterstützt virtuellen Server**
  Ermöglicht Internet-Benutzern den Zugang auf WWW, FTP und anderen Diensten in Ihrem LAN.
- **Benutzerdefinierbarer Abtasttunnel für Anwendungen**
  Benutzer können Attribute definieren, um Sonderanwendungen zu unterstützten, die mehrfache Verbindungen benötigen, z.B. Spiele im Internet, Videokonferenzen, Internet-Telefonie und so weiter, denn dieses Produkt kann den Anwendungstyp abtasten und dafür einen Multi-Porttunnel öffnen.
- **Unterstützter DMZ-Host**
  Hiermit wird ein vernetzter Computer im Internet komplett sichtbar; diese Funktion wird verwendet, wenn der Abtasttunnel für Anwendungen für ein richtiges Funktionieren der Anwendung nicht ausreicht.
- **Unterstützte WAN-Statistik**
  Ermöglicht Ihnen die Überwachung von ein- und ausgehenden Paketen.

Drahtlosfunktionen

- **Hochgeschwindigkeit für Drahtlos-LAN-Verbindung**
  Datenübertragungsrate bis zu 80 Mbit/s durch Einbindung von OFDM (Orthogonal Frequency Division Multiplex, Orthogonales Frequenztrennungs-Multiplex-Verfahren).
- **Roaming**
  Bietet nahtloses Roaming innerhalb einer IEEE 802.11b- (11M) und IEEE 802.11g- (54M) WLAN-Infrastruktur.
- **WDS (**Wireless Distribution System, Drahtloses Verteilungssystem von Verbindungen**):** Es handelt sich hier um System, das die drahtlose Querverbindung von Zugangspunkten (Access Point, AP) ermöglicht.
- **WPS (**WiFi Protected Setup, WiFi-geschützte Einrichtung**):** WPS steht für WiFi Protection Setup, was dem WCN-NET ähnelt und eine sichere und einfache Methode für drahtlose Verbindungen bietet.
- **IEEE 802.11b-kompatibel (11M)**
  Ermöglicht einen übergreifenden Betrieb von Geräten unterschiedlicher Hersteller.
- **IEEE 802.11b-kompatibel (54M)**
  Ermöglicht einen übergreifenden Betrieb von Geräten unterschiedlicher Hersteller.
- **IEEE 802.11n-kompatibel (300M)**

“Grüne” Funktionen

- **Standby-Modus:**
  Wird dem “grünen” Router innerhalb von einigen Minuten keine Drahtlosstation zugewiesen, wird automatisch in den Standby-Modus gewechselt. Dieser Modus hat natürlich keinen Einfluss auf das Roaming von Endbenutzern im Internet, z.B. Reset 12:00~13:30 zur Mittagszeit.

- **Ruhemodus:**
  Sobald die Zeit mit der programmierten Regelzeit übereinstimmt, ermittelt der “grüne” Router, ob ein Datenverkehr auf dem Client oder im Netzwerk stattfindet. Falls nicht, wechselt der “grüne” Router in den Ruhemodus. Er wechselt nur dann in den Ruhemodus, wenn kein Datenverkehr mehr im Netzwerk stattfindet. In diesem Modus kann beinahe 100% an Energie eingespart werden. (Endbenutzer bekommen im Ruhemodus keinen Zugriff auf das Internet.) Zum Beispiel von 23.00 Uhr ~ 10.00 Uhr für die Familie oder von 19.00 Uhr ~ 07.00 Uhr für das Büro oder am Wochenende.

- **Smarter Zeitplan:**
  Sobald die Zeit mit der programmierten Regelzeit übereinstimmt, z.B. von 23.00 Uhr ~ 08.00 Uhr wird der Ruhemodus aktiviert, ermittelt der “grüne” Router um 23.00 Uhr, ob ein Datenverkehr im Netzwerk oder in den Drahtlosstationen stattfindet; wenn nicht, wechselt er bis 08.00 Uhr in den Ruhemodus. Falls doch, erkundet der “grüne” Router solange, bis kein Datenverkehr mehr im Netzwerk oder auf den Drahtlosstationen stattfindet, und wechselt dann in den “Ruhemodus”.
  Der smarte Zeitplan hat noch eine weitere Funktion: Wenn der Endbenutzer um 3.00 Uhr aufwacht, dann die Schaltfläche On/Sleep (Ein/Ruhezustand) anklickt und bis 5.00 Uhr im Internet surft, erkennt der “grüne” Router, dass ab diesem Zeitpunkt kein Datenverkehr mehr im Netzwerk oder auf den Drahtlosstationen stattfindet, und wechselt dann bis 8.00 Uhr in den “Ruhemodus”.

- **Schaltfläche On/Sleep (Ein/Ruhezustand):**
  Mit dieser Schaltfläche lässt sich der “grüne” Router aus dem Ruhemodus aufwecken.

  ※ Es gibt eine Einschränkung für den Endbenutzer hinsichtlich der Erzwingung des Ruhezustands mit dieser Schaltfläche, auch muss der "grüne" Router mit dieser Schaltfläche wieder aufgeweckt werden. Mit dieser Schaltfläche wird das Gerät zum Aufwecken gezwungen und es kann per Zeitplan in den Ruhemodus wechseln.

Sicherheitsfunktionen

- **Unterstützter Paketfilter**
  Packet Filter (Paketfilter) ermöglicht Ihnen, den Zugang zu einem Netzwerk durch Analyse von ein- und ausgehenden Paketen so zu kontrollieren, dass sie auf Basis der IP-Adresse der Quelle und des Zieles entweder passieren dürfen oder gestoppt werden.
- **Unterstützter Domänenfilter**
  Hiermit verhindern Sie, dass Benutzer dieses Geräts auf bestimmte URLs zugreifen.
- **Unterstützte URL-Blockierung**
  Mit URL Blocking (URL-Blockierung) lassen sich Hunderte von Website-Verbindungen auf einfache Weise mit einem **Schlüsselwort** blockieren.
- **VPN-Einbindung (an ein virtuelles privates Netzwerk)**
  Dieser Router unterstützt auch die VPN-Einbindung (Virtual Private Network, Virtuelles privates Netzwerk).
- **Unterstützt 802.1X**
  Bei aktivierter 802.1X-Funktion muss der Drahtlosbenutzer zuerst diesen Router authentifizieren, um den Netzwerkdienst zu verwenden.
- **Unterstützt WPA-PSK und WPA Version 1 und 2**
  Bei aktivierter WPA-Funktion (WiFi Protected Access, WiFi-geschützter Zugang) muss der Drahtlosbenutzer zuerst diesen Router authentifizieren, um den Netzwerkdienst zu verwenden.
- **Unterstützte SPI-Modus**
  Bei aktiviertem SPI-Modus (Serial Peripheral Interface, Serielle Peripheriegerät-Schnittstelle) prüft der Router jedes eingehende Paket auf Gültigkeit.
- **Unterstützt DoS-Angriffsmeldung (Denial of Service, Dienstverweigerung)**
  Wenn diese Funktion aktiviert ist, meldet und protokolliert der Router einen DoS-Angriff vom Internet.
- **QoS (Quality of Service, Dienstgüte)**
  Gibt unterschiedlichen Benutzern oder Datenströmen unterschiedliche Prioritäten oder garantiert einen bestimmten Leistungsgrad.

Erweiterte Funktionen

- **Unterstützte Systemzeit**
  Ermöglicht die Synchronisierung der Systemzeit mit dem Netzwerkzeitserver.
- **Unterstützt E-Mailwarnung**
  Der Router sendet Informationen per E-Mail.
- **Unterstützt dynamisches DNS (Domänennamesystem)**
  Derzeit unterstützt der Router einige DDNS-Anbieter wie “Dyndns”, “TZO.com” ohne IP und “Dhs.org”.
- **Unterstütztes SNMP (Simple Network Management Protocol, Einfaches Netzwerkverwaltungsprotokoll)**
  Dieser Router unterstützt eine grundlegende SNMP-Funktion.
- **Unterstützt Routingtabelle**
  Der Router unterstützt jetzt auch statisches Routing.
- **Unterstützt Programmierung der Regelzeit**
  Benutzer können kontrollieren, wann ein Zugriff auf Funktionen wie virtueller Server und Paketfilter möglich ist und wann diese blockiert werden.

Weitere Funktionen

- **Unterstützt UPNP (Universal Plug and Play, Universelles Plug-and-Play)**
  Dieser Router unterstützt auch diese Funktion. Die Anwendungen: X-box (360), MSN Messenger, Windows Messenger und NDSL.

Lieferumfang

Öffnen Sie den Karton des *HomeGuard 22 Residential Gateways* und packen Sie ihn vorsichtig aus. Folgende Gegenstände sollten im Karton enthalten sein:

- WBR-6022 *HomeGuard 22 Residential Gateway*
- Netzteil
- Kabel der Kategorie 5
- Antenne, x 2
- CD-Handbuch / Dienstprogramm
- Anleitung für Kurzinstallation

Sollte eines der Gegenstände fehlen oder beschädigt sein, bitten Sie Ihre Verkaufsstelle vor Ort um Ersatz.

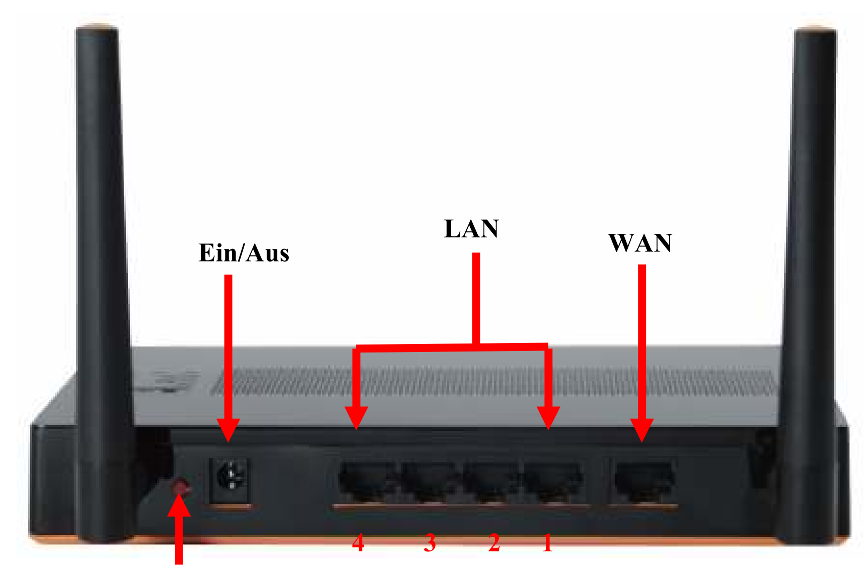
3 Hardware-Installation

Vorderseite



WLAN-Taste	• Drücken und 3 Sekunden lang halten, um das Drahtlos-LAN ein- oder auszuschalten. • Bestätigen Sie den WLAN-Status gemäß WLAN-Anzeige
Statusanzeige	• Eine durchgehend blinkende Anzeige bedeutet, dass das Gerät betriebsbereit ist.
WAN-Anzeige	• Eine leuchtende Anzeige bedeutet, dass der WAN-Anschluss verbunden ist.
WAN-Anzeige	• Wenn diese Anzeige nicht leuchtet, ist das Drahtlos-LAN ausgeschaltet oder es ist kein Drahtlos-Client mit dem Router verbunden. • Diese LED blinkt während einer drahtlosen Datenübertragung oder, wenn ein Drahtlos-Client mit dem Router verbunden ist. • Eine durchgehend schnell blinkende Anzeige bedeutet, dass die WPS-Funktion aktiviert ist und der Router sich mit einem Drahtlos-Client koppelt.
LAN-Anzeige	• Eine leuchtende Anzeige bedeutet, dass ein Ethernet-aktivierter Computer mit den Anschlüssen 1 ~ 4 verbunden ist. • Diese LED blinkt während einer Datenübertragung.
Ruhemodusanzeige	• Eine (orange) leuchtende Anzeige bedeutet, dass sich der Router im Ruhemodus befindet.
WPS-Taste	• Taste für Wi-Fi Protected Setup (Wi-Fi-geschütztes Setup). Wenn Sie diese drücken, aktiviert sich die WPS-Kopplung mit dem Drahtlos-Client.
Reset (WLAN- und WPS-Tasten)	• Drücken und halten Sie die Tasten WLAN und WPS gleichzeitig 5 Sekunden lang, um das Gerät neu zu starten und es auf die werkseitigen Standardeinstellungen zurückzusetzen.

Rückseite



Netzanschluss	• Anschluss für das mitgelieferte Netzteil.
LAN-Anschlüsse (1~4)	• Verbindet Ethernet-Geräte wie Computer, Switch oder Hub.
WAN-Anschluss	• Der WAN-Anschluss verbindet das Ethernet-Kabel mit dem Kabel- oder DSL-Modem.
Taste Ruhezustand	• Mit dieser Taste wird der Router in den Ruhemodus versetzt oder wieder aktiviert. Sie hat die höchste Priorität und setzt den Zeitplan für Energieeinsparung außer Kraft. • Der “grüne” Router befindet sich im Ruhemodus. (Halten Sie diese Taste ca. 1 Sekunde lang gedrückt.) • Der “grüne” Router befindet sich im Standby-Modus oder er ist eingeschaltet. (Halten Sie diese Taste ca. 1 Sekunde lang gedrückt.)
Antennen	• Abnehmbare Antennen können vom Benutzer ausgetauscht werden, falls erforderlich.

Hardware-Installation

Bestimmen Sie, wo Sie Ihren Dratlos-Router aufstellen möchten

Sie können Ihren Drahtlos-Router auf einen Tisch oder eine andere flache Oberfläche stellen. Eine optimale Leistung erzielen Sie, wenn Sie Ihren Drahtlos-Router an einen Ort in der Mitte Ihres Büros (oder Ihrer Wohnung) aufstellen, in dessen Nähe sich keine potentiellen Störquelle befinden, wie z.B. eine Wand aus Metall oder ein Mikrowellenherd. In der Nähe dieses Aufstellungsortes muss sich auch eine Steckdose und ein Netzwerkanschluss befinden.

1. Bringen Sie die beigefügten Antennen an.



2. Verbinden Sie Ihr Breitband-Internet mit dem WAN-Anschluss des WBR-6022.



3. Schließen Sie das Computer-LAN-Kabel an.



4. Schließen Sie das Netzteil an.



5. Warten Sie, bis die Statusanzeige durchgehend blinkt.
Dies bedeutet, dass der Router betriebsbereit ist.

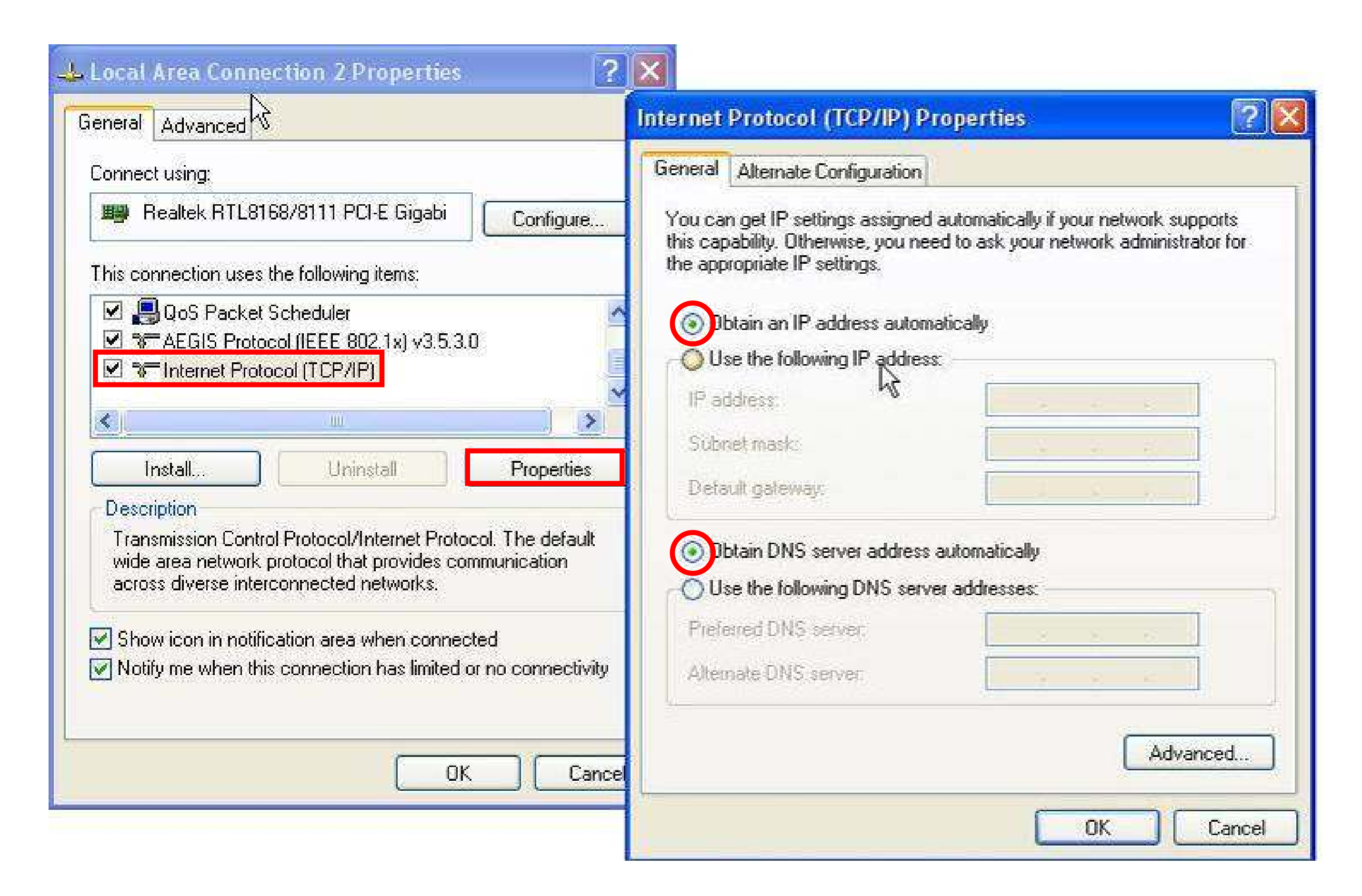


6. Verbinden Sie die IP-Kamera(s) & FNS-1020v2 für das Üverwachungssystem. Bitte beachten Sie das folgende Anwendungsbeispiel.



4 Prüfen der Netzwerkeinstellungen

1. Vergewissern Sie sich, dass Ihr PC die IP-Adresse automatisch bezieht, so dass der WBR-6022 während der Konfiguration mit Ihrem PC kommunizieren kann.
   - Wählen Sie “Control Panel” (Systemsteuerung) > “Network Connections” (Netzwerkverbindungen).
   - Klicken Sie mit der rechten Maustaste auf “Local Area Connection” (LAN-Verbindung) und wählen Sie “Properties” (Eigenschaften).
   - Wählen Sie das TCP/IP-Protokoll für Ihre Netzwerkkarte.
   - Klicken Sie auf die Schaltfläche “Properties” (Eigenschaften). Sie sollten dann den folgenden Bildschirm sehen; vergewissern Sie sich, dass Sie “Obtain IP address automatically” (IP-Adresse automatisch beziehen) gewählt haben.



2. Starten Sie Ihren Computer neu, damit sichergestellt wird, dass Sie die IP-Adresse richtig erhalten haben.

5 Einrichtung des WBR-6022 Überwachungssystem

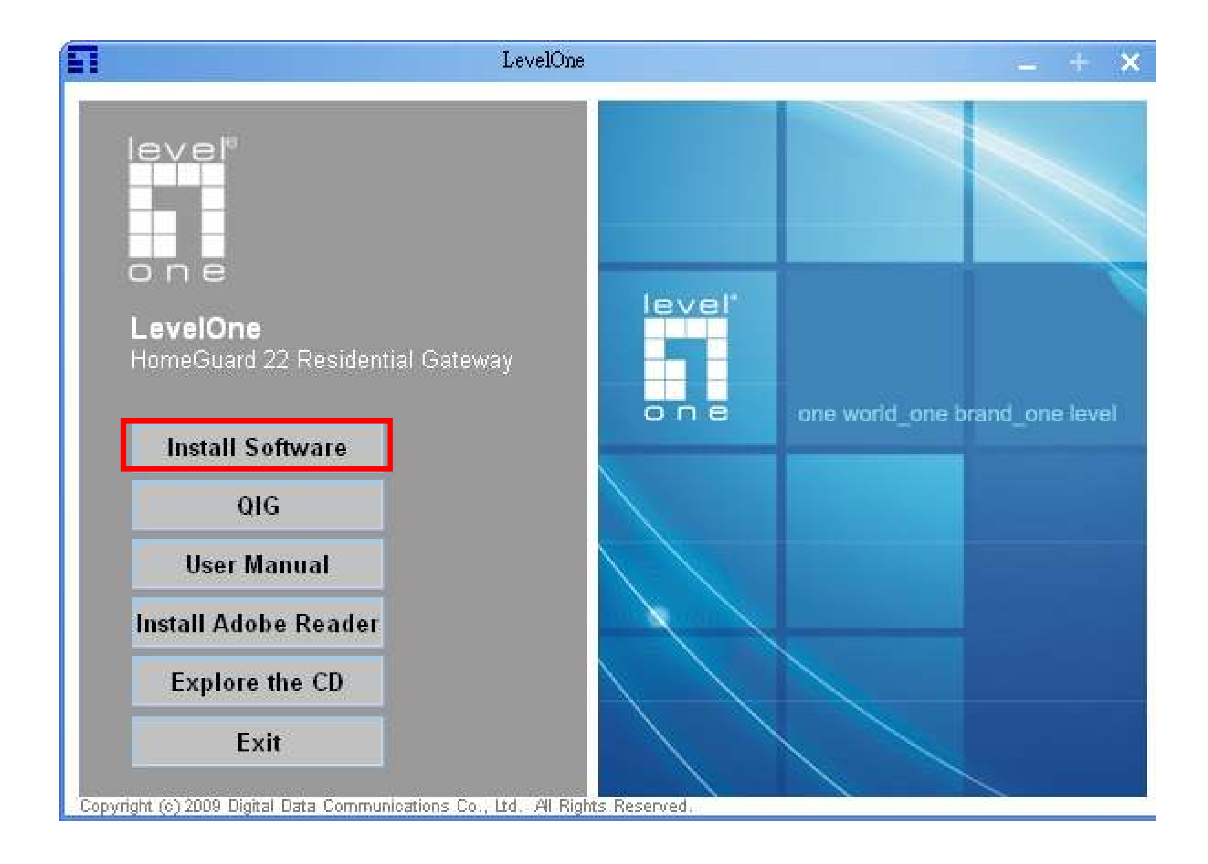
Sobald der WBR-6022 *HomeGuard 22 Residential Gateway* richtig konfiguriert ist, wird er IP-Adressinformationen automatisch beziehen und zuweisen. Konfigurationseinstellungen können über das Web-basierte Menü oder das Dienstprogramm Easy Setup (Schnelle Einrichtung) auf der CD eingerichtet werden.

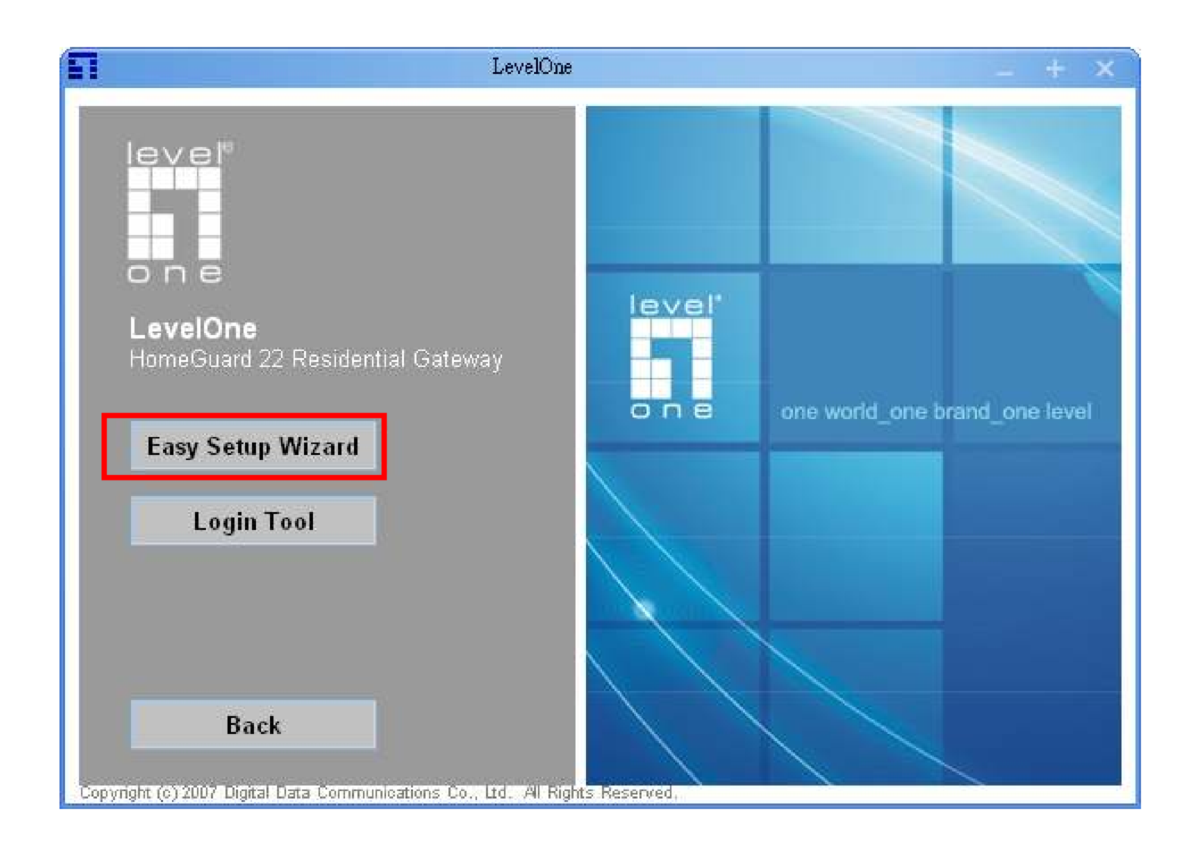
5.1 Das Easy Setup Dienstprogramm (Schnelle Einrichtung)

Legen Sie die CD in das CD-ROM-Laufwerk Ihres Computers.

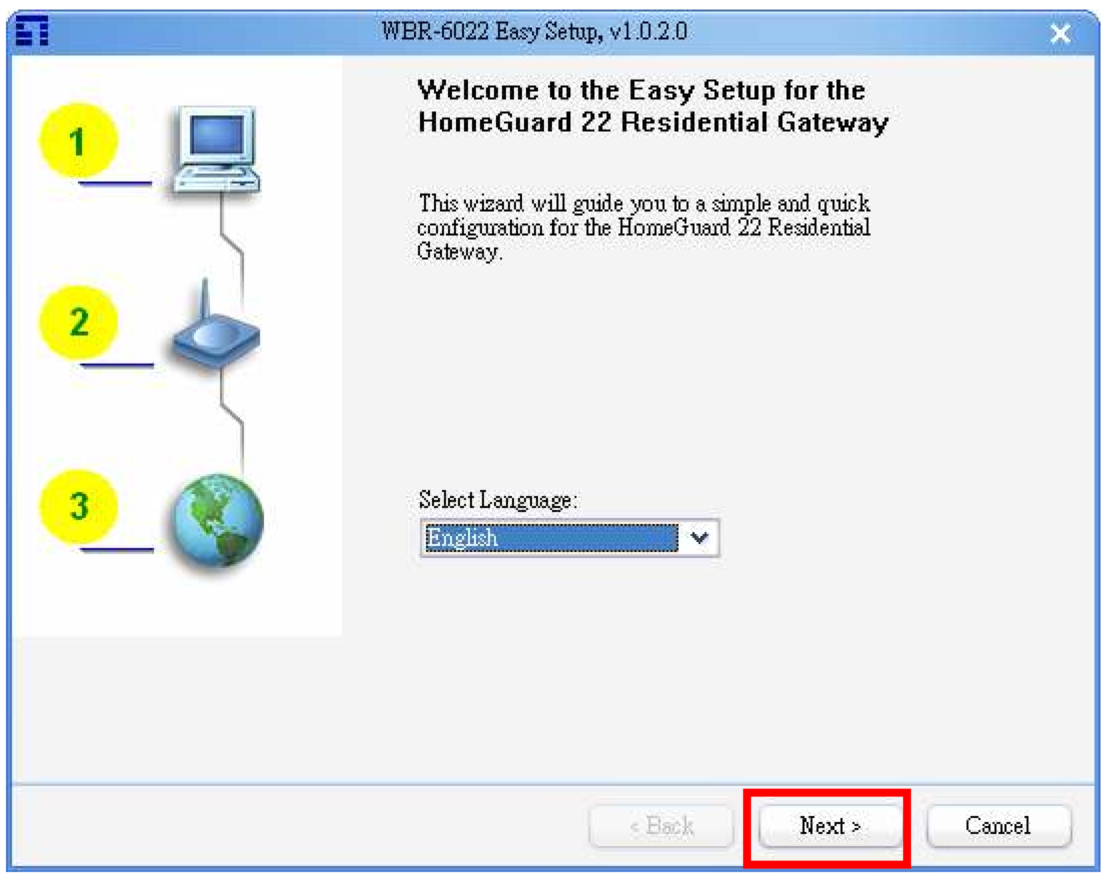
Das Autorun-Programm sollte automatisch starten.
Falls nicht, führen Sie die Datei “autorun.exe” auf Ihrer CD aus.

Klicken Sie im Autorun-Bildschirm auf ***Utility (Dienstprogramm)***, um mit Easy Setup (Schnelle Einrichtung) zu beginnen.



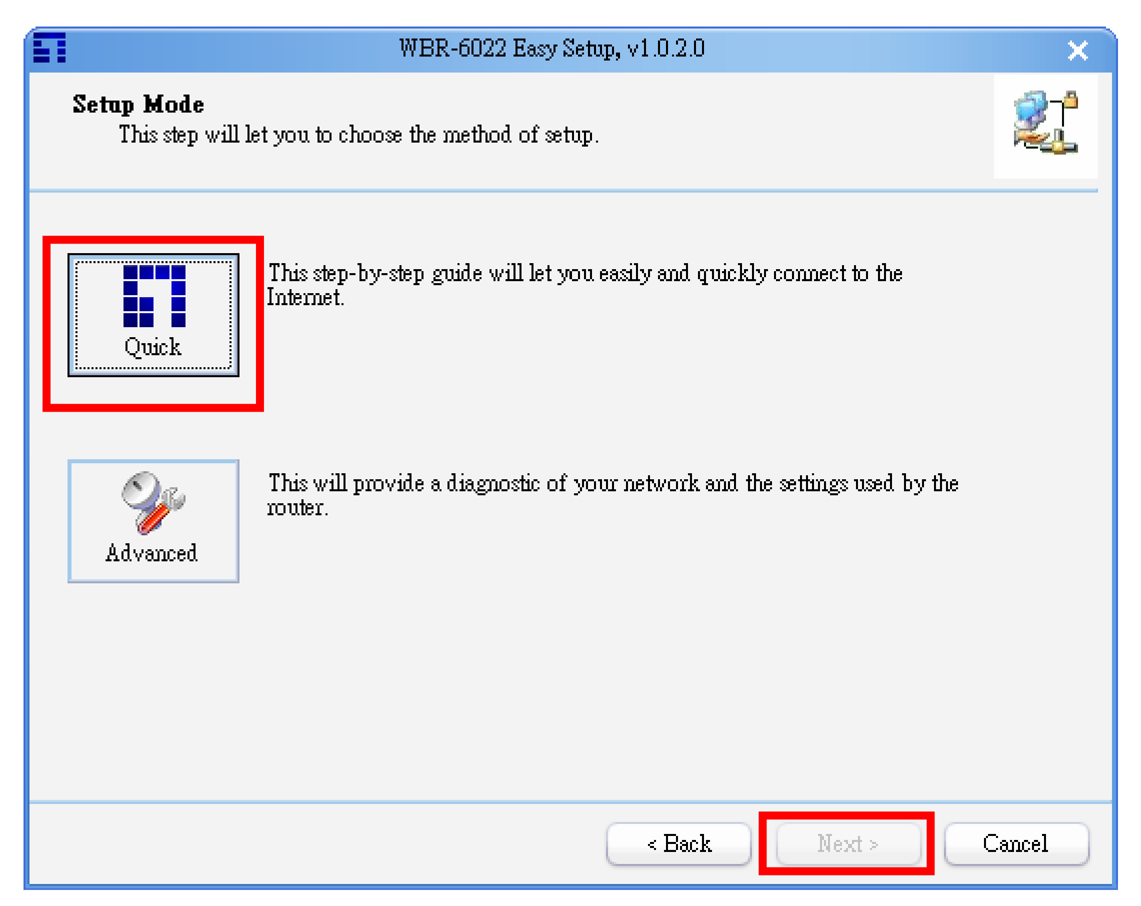


Vor Ausführung von Easy Setup (Schnelle Einrichtung) muss gewährleistet sein, dass Ihr PC ordnungsgemäß mit dem Router verbunden ist. Nach der Ausführung dieses Programms sollten Sie folgenden Bildschirm sehen:

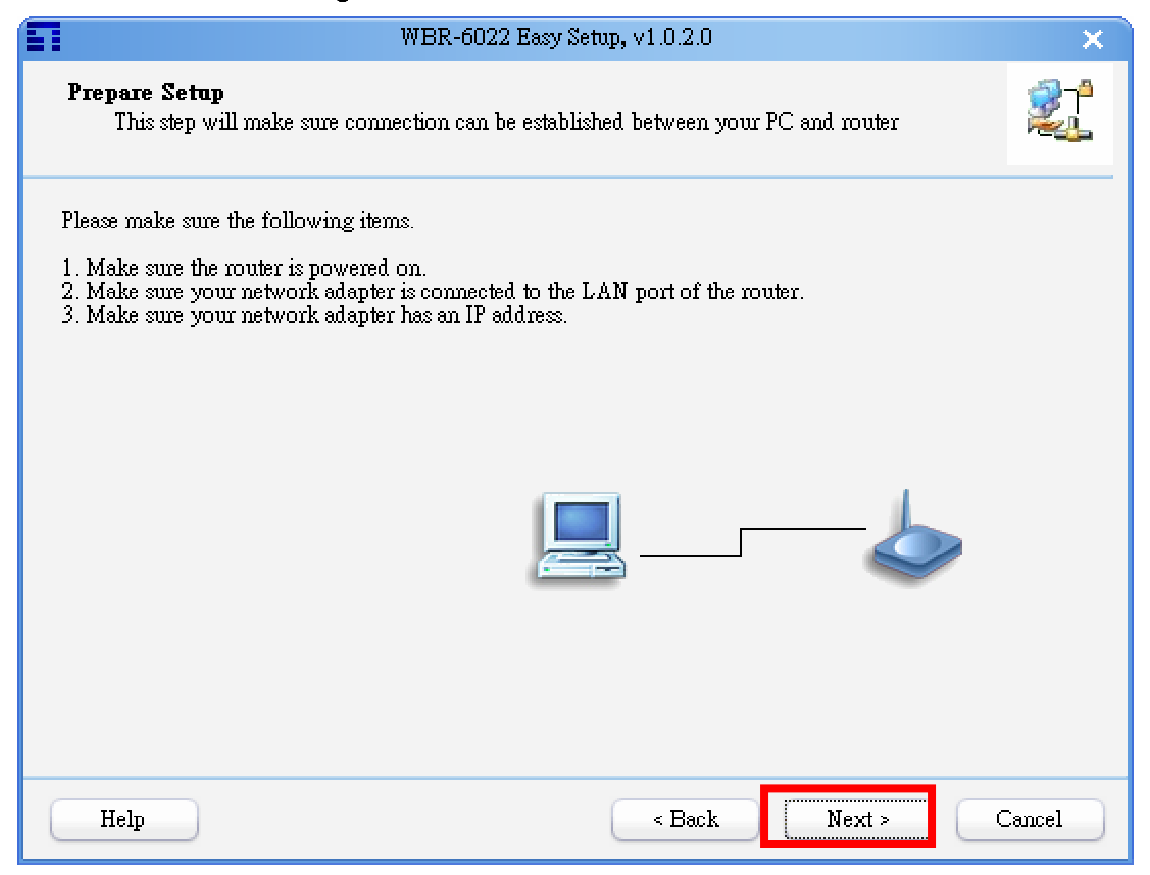


Wählen Sie die Sprache des Easy Setup-Installationsassistenten aus.

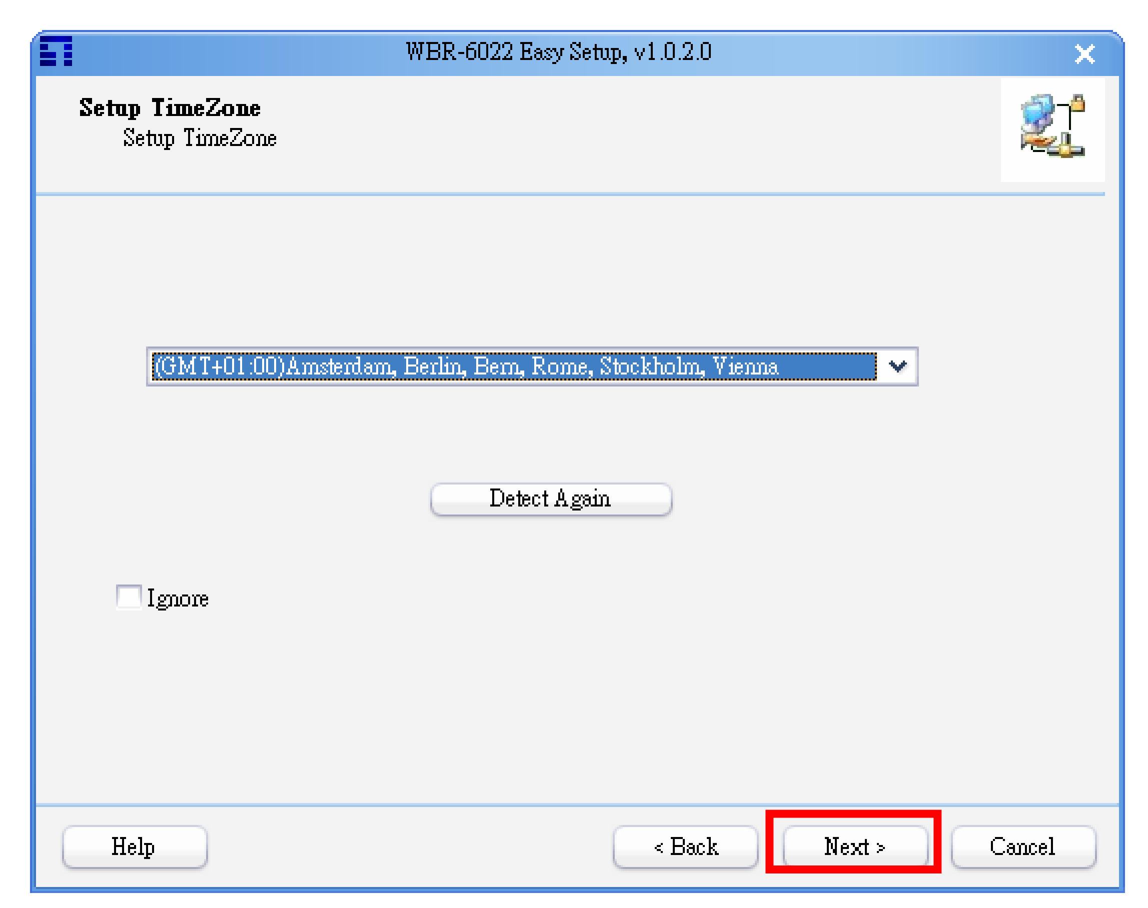
Klicken Sie auf “**Next**” um fortzufahren.



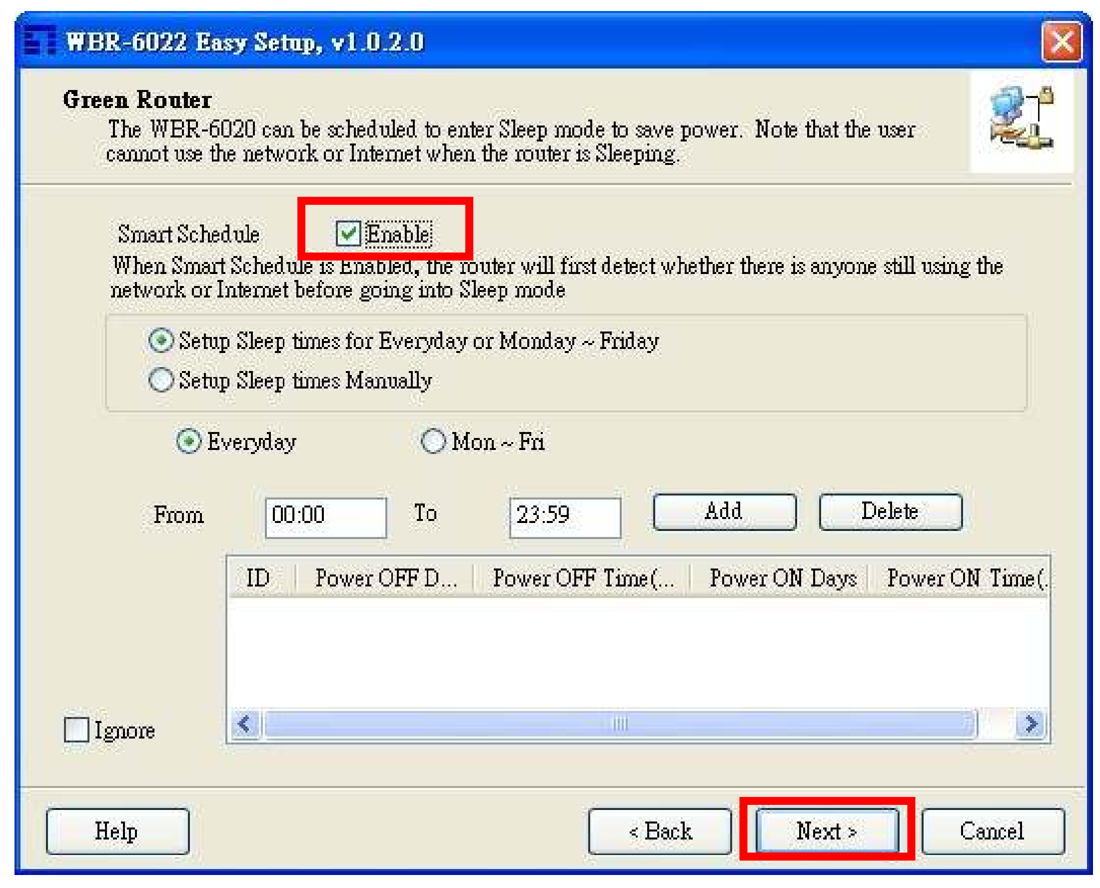
Wählen Sie den Quick-Installationsassistenten aus, der Sie schrittweise durch die Konfiguration führen wird. Klicken Sie auf “**Next**” um fortzufahren.



Stellen Sie sicher, dass Ihre Hardware-Verbindungen korrekt angeschlossen sind. Klicken Sie auf “**Next**” um fortzufahren.

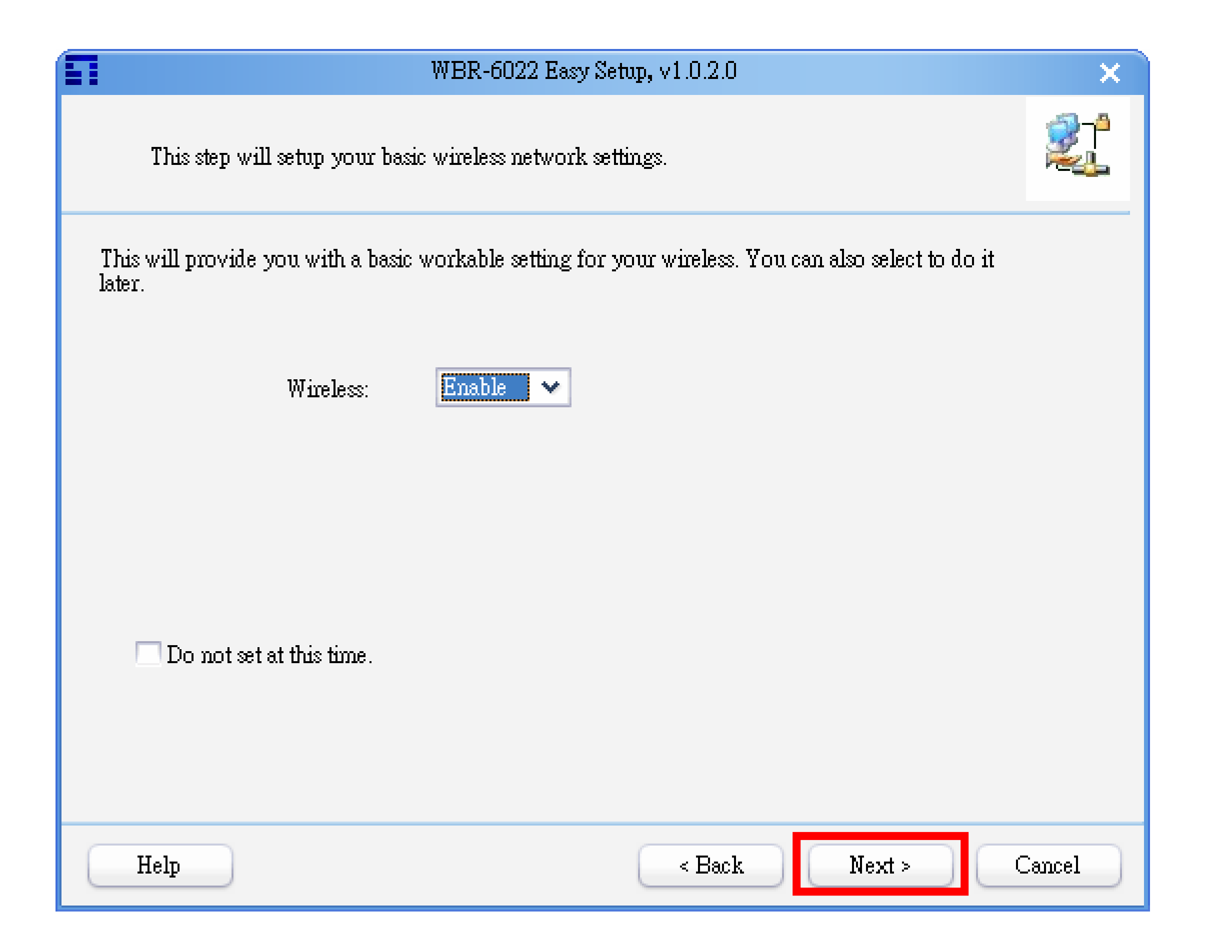


Sie müssen dann die Zeitzone einstellen. Dieser Router verwaltet die Energie eventuell nach einem Zeitplan, so dass Sie die Systemzeit berichtigen müssen. Klicken Sie auf "**Next**" um fortzufahren.

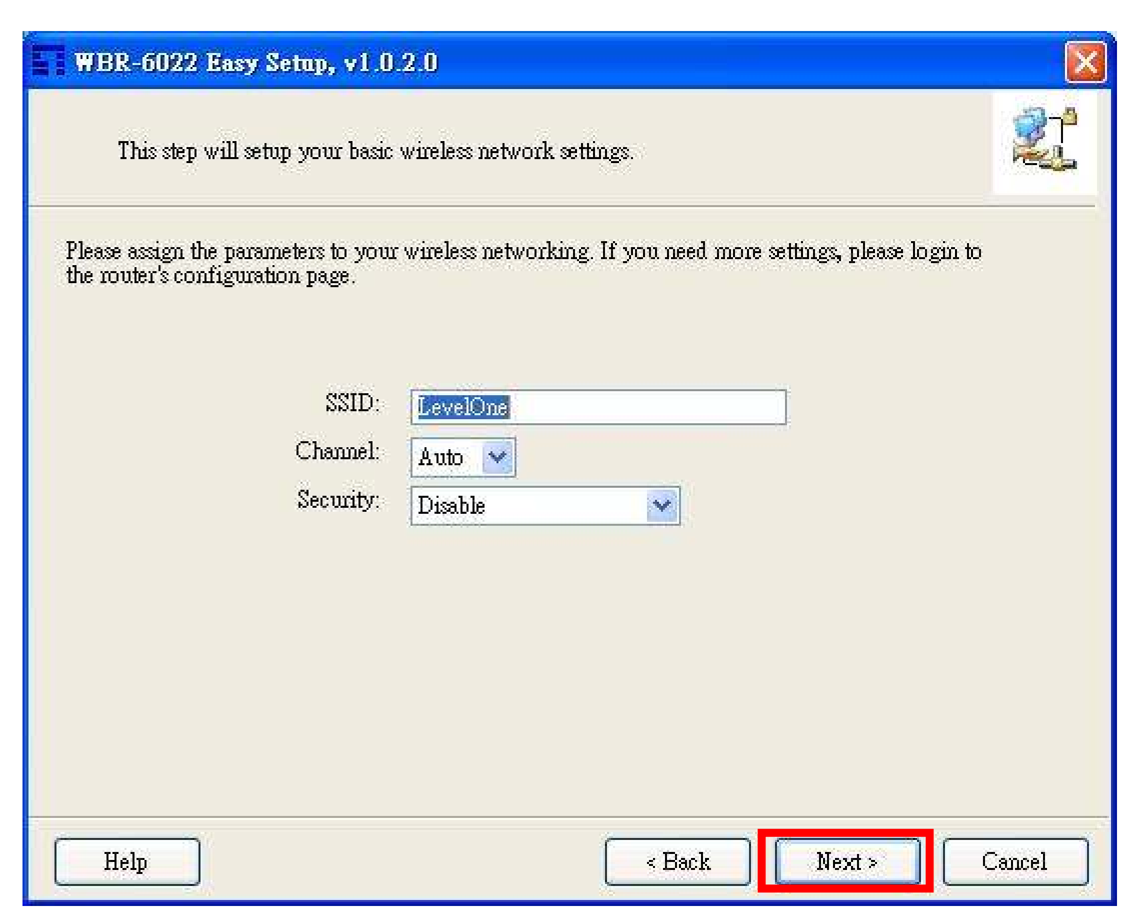


Klicken Sie auf "**Enable**" Smart Schedule und dann auf "**Next**".

Smart Schedule bedeutet, dass wenn der Router aufgrund der programmierten Regelzeit in den Ruhemodus wechseln soll, er zuerst das Netzwerkpaket überprüft. Sollten zu diesem Zeitpunkt weiterhin Netzwerkpakete übertragen werden, wird die Regel nicht sofort ausgeführt, sondern erst dann, wenn im Netzwerk kein Datenverkehr mehr stattfindet.



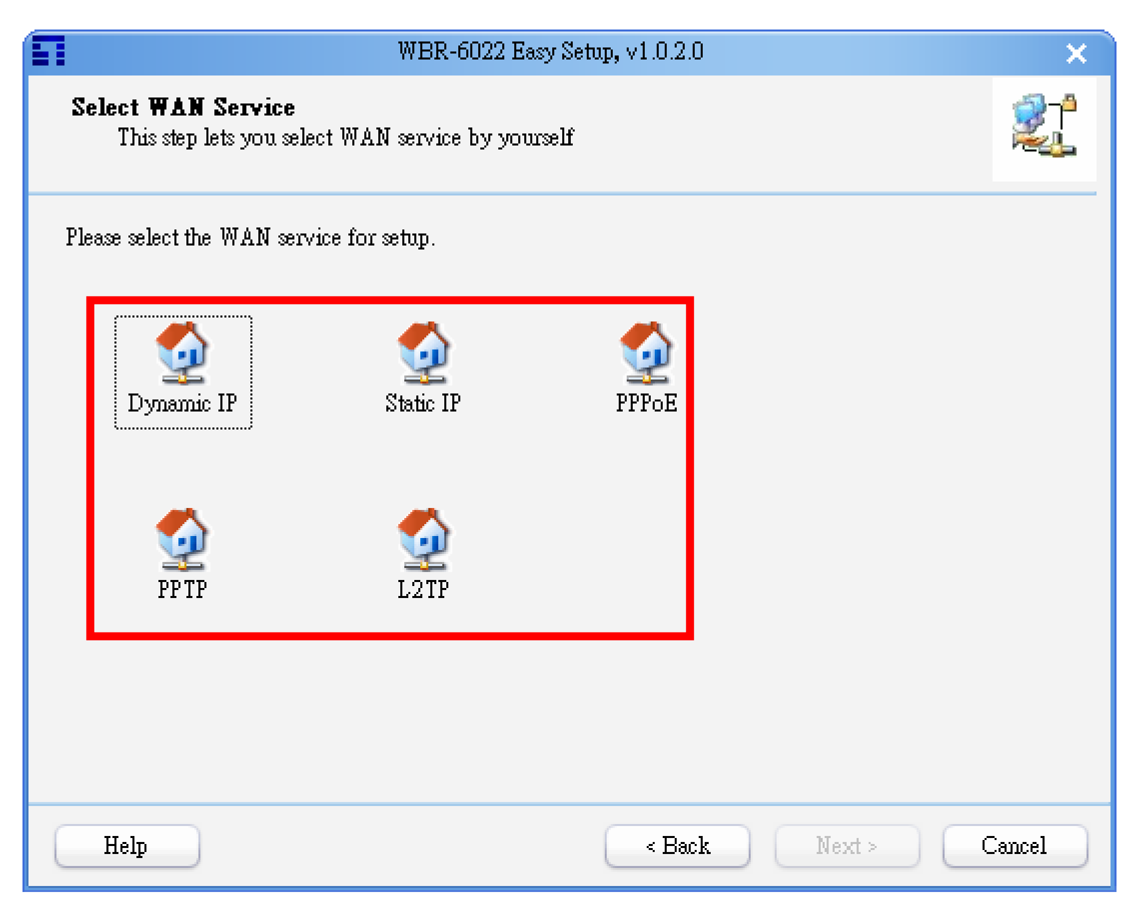
Aktivieren oder deaktivieren Sie die Wireless Funktion.
Klicken Sie auf “**Next**” um fortzufahren.



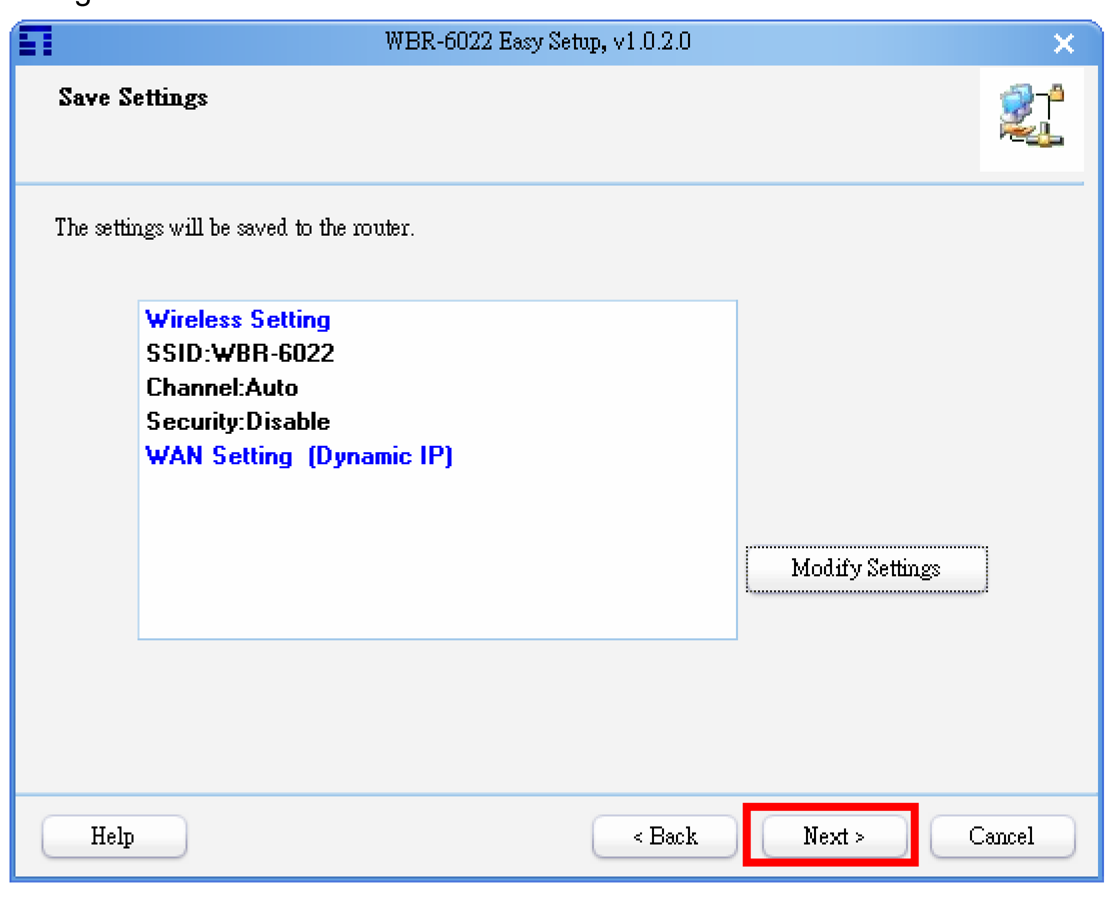
Für die Drahtloseinstellungen des "HomeGuard" ist die Standard-SSID "LevelOne", der Standardkanal ist "11" und die Standardverschlüsselung ist auf "NONE" (Nichts) gesetzt. Sie können diese Einstellungen jetzt oder später über die Weboberfläche ändern. Wir raten Ihnen dringendst, die Verschlüsselungsoption möglichst bald zu ändern, denn ein unverschlüsseltes Drahtlosnetzwerk ist nicht sicher. Klicken Sie auf "**Next**" um fortzufahren.



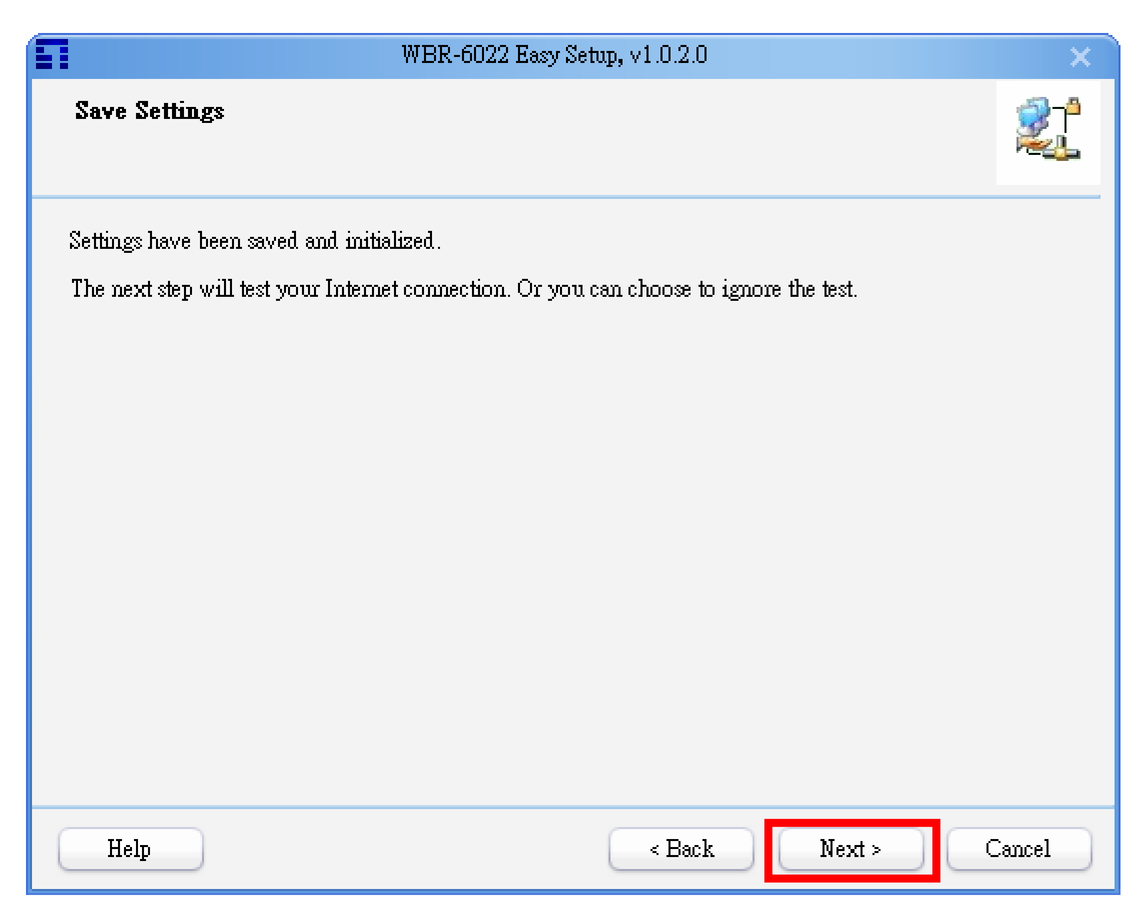
Klicken Sie auf “**Next**” um fortzufahren.



Im nächsten Schritt helfen wir Ihnen bei der Einrichtung der WAN-Konfigurationen. Folgen Sie dem Assistenten und wählen den von Ihnen verwendeten WAN-Typ aus.



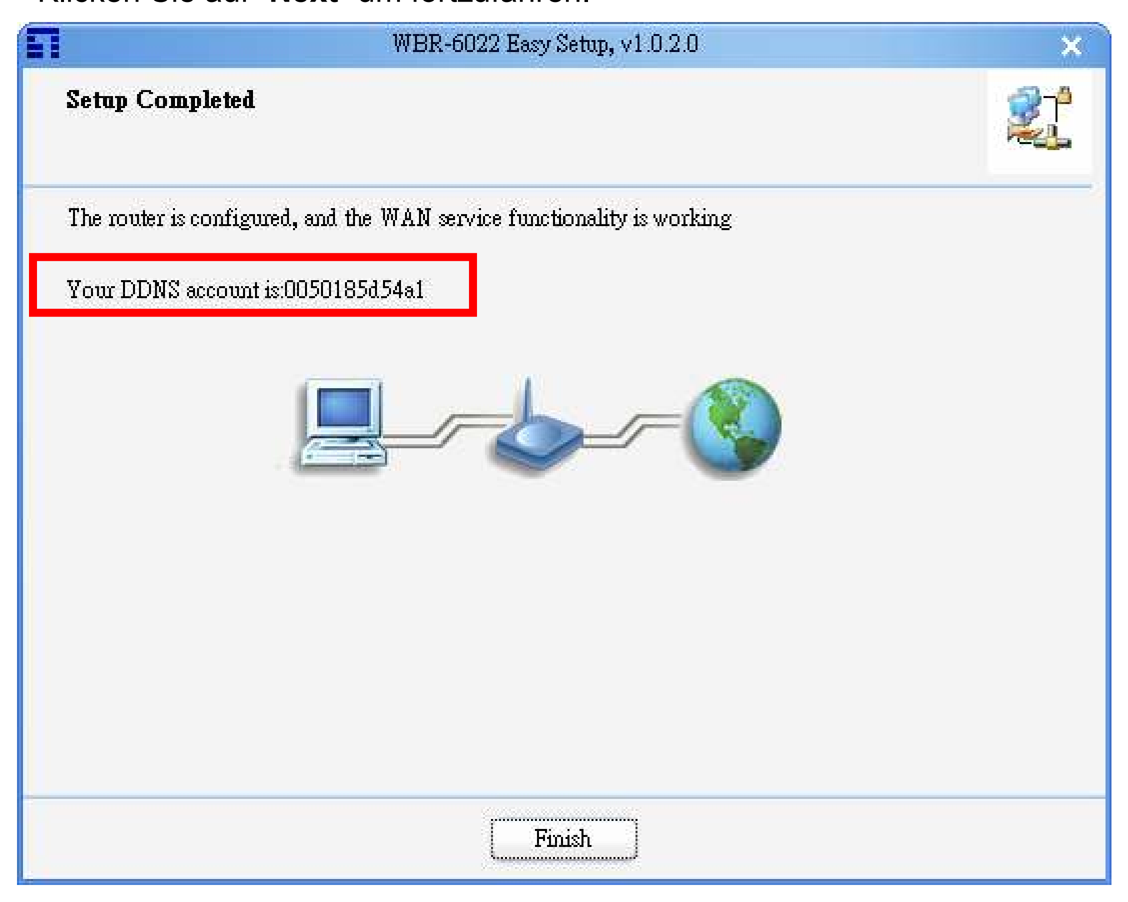
Klicken Sie auf “**Next**” um fortzufahren.



Klicken Sie auf “**Next**” um fortzufahren.



Testen Sie nun WBR-6022's Level1DNS-Verbindung und Account-Namen. Klicken Sie auf "**Next**" um fortzufahren.



Die Anwendung zeigt Ihnen einen Standard-Domain-Namen, der diesem Produkt zugeordnet ist und den Sie nicht vergessen dürfen. Wenn Sie dieses HomeGuard-System beim nächsten Mal von der Ferne aus steuern möchten, können Sie sich mit diesem Domain-Namen anmelden. Da dieser nicht leicht zu merken ist, können Sie einen von Ihnen bevorzugten Domain-Namen auf der Weboberfläche einstellen.

Das Standard-Format ist Level1DNS "Alias-Name oder MAC-Adresse" + "level1dns.net". Sie können Ihren bevorzugten Alias-Namen auch später über das Web-UI ändern.

Beispiel: Das Level1DNS Konto kann "01150185d54a1" sein, somit ist Ihr kompletter DDNS Domain-Name: "00116b5d54a1.level1dns.net".

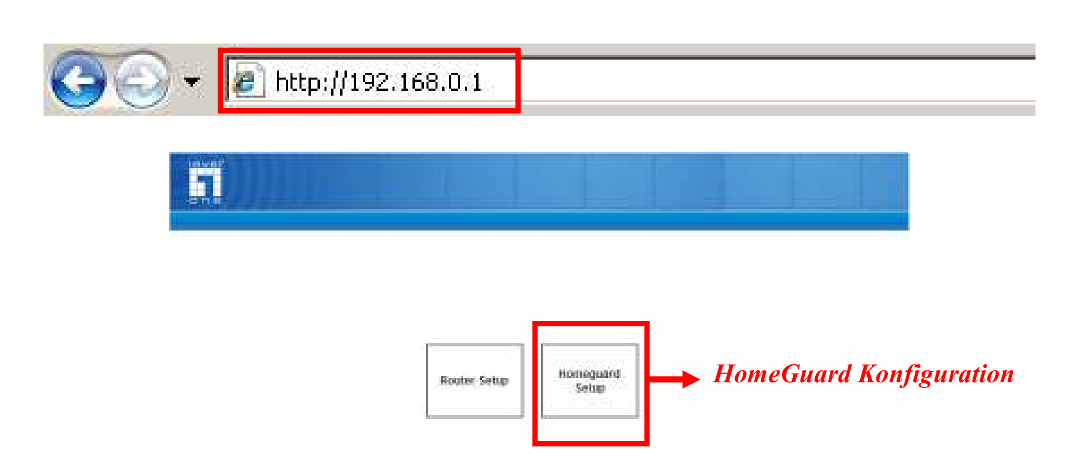
6 Einfache Konfiguration des HomeGuard-System

Für die Konfiguration des HomeGuard-System benötigen Sie nur wenige Schritte, um alle Einstellungen vorzunehmen:

1. Verbinden Sie alle IP-Kameras und FNS-1020v2 mit dem WBR-6022, dann schalten Sie alle Geräte an.
2. Stellen Sie sicher, dass der WBR-6022 mit dem Internet verbunden ist (sofern Sie die IP-Kamera-Funktion nutzen möchten).
3. Drücken Sie die WPS-Taste des WBR-6022 für 5 Sekunden.
4. Drücken Sie die WPS-Taste der IP-Kamera(s) für 5 Sekunden und warten Sie bitte 20 Sekunden ab. (Schritt 3 und 4 sind optional.)
5. Suchen Sie nach neuen Geräten und registrieren Sie jedes davon.
6. Ändern Sie den Namen eines jeden Gerätes, falls dies notwendig ist.
7. Ändern Sie den bevorzugten Domain-Name des WBR-6022 auf dem Level1DNS-Service.
8. Führen Sie die Aufnahme-Einstellungen durch, wenn Sie die FNS-1020v2 registriert haben.
9. Sehen Sie sich das Video der registrierten IP-Kamera(s) an.
10. Wiedergabe: Wenn Sie eine FNS-1020v2 installiert haben, können Sie Videos aufnehmen und wiedergeben.

6.1 HomeGuard Konfiguration

A.



Öffnen Sie Ihren IE-Browser und geben die IP-Adresse http://192.168.0.1 ein.
(Das Active-X arbeitet nur mit IE.)

B.



Klicken Sie auf **"Login".**
(Der Standard-Username und Passwort ist "**admin**" und "**password**".)

C.

Startseite

Multiple Sprachauswahl

Hauptfunktionen

English

Home Logout

Status

Search New Device

Schedule

System

IP Camera

Cam Recorder

Welcome, admin

March 17
2010

Status

Help

IP Camera

Item	Status	Setup

NVR

Item	Status	Setup

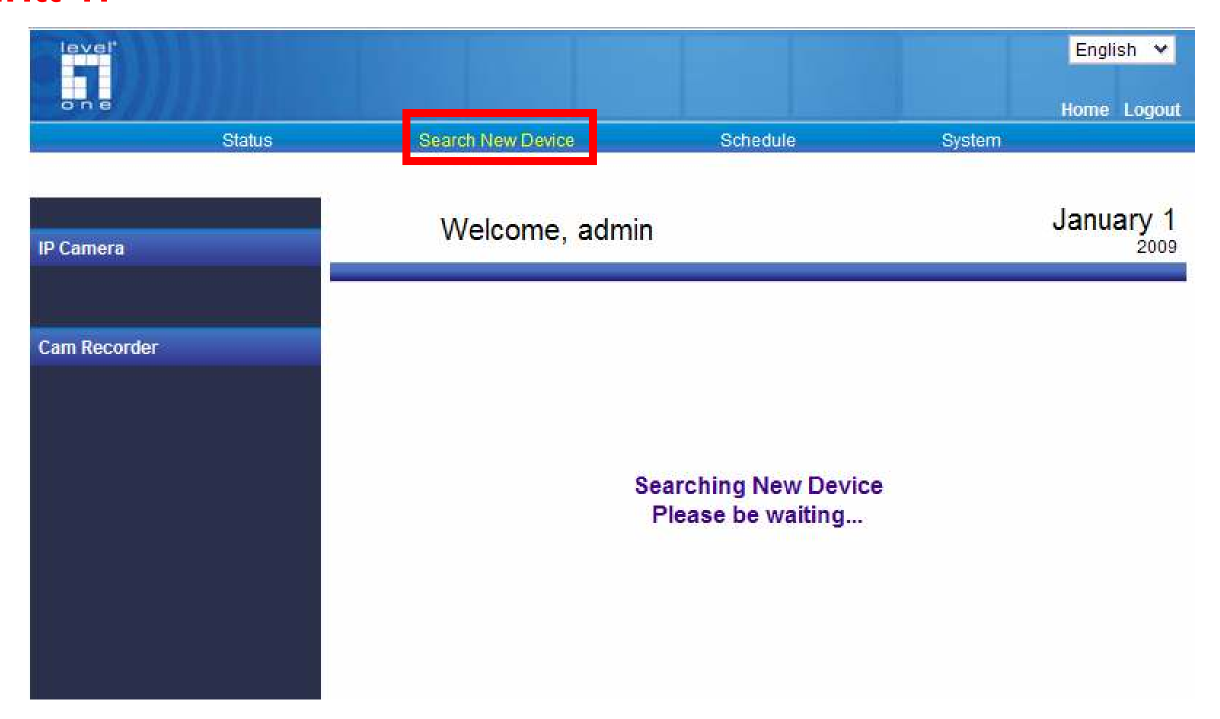
IP Geräte Liste

Online Hilfe

6.1.2 Suche nach neuen Geräten

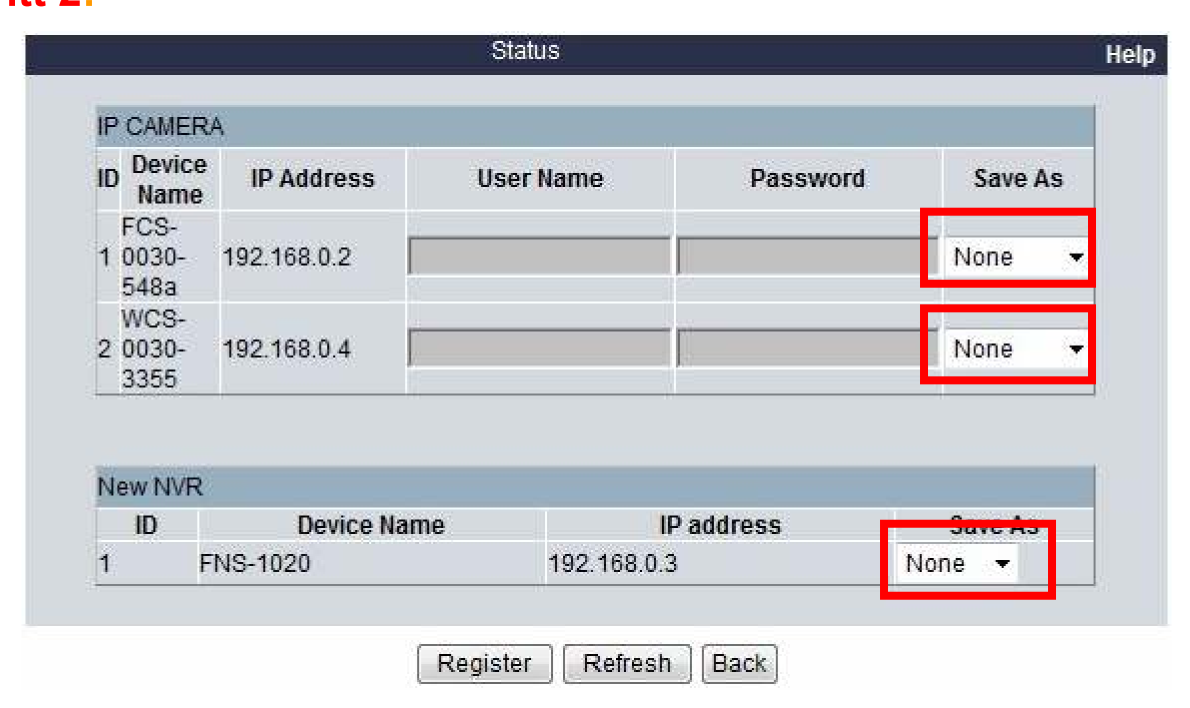
Klicken Sie auf das **"Search New Device"**-Icon, damit das HomeGuard-System nach allen IP-kompatiblen Geräten suchen kann, die mit dem WBR-6022 verbunden sind.

Schritt 1:



Klicken Sie auf **"Search New Device"**.

Schritt 2:



Wählen Sie IPCam1 / IPCam2 / NVR1 aus.

Modell-Name & Username / Passwort

Model Name	Username / Password
FCS-0010 / WCS-0010	Standard-Username ist “**administrator**” und das Passwort-Eingabefeld bleibt leer.
FCS-0020 / WCS-0020	Standard-Username ist “**administrator**” und das Passwort-Eingabefeld bleibt leer.
FCS-1030v2 / WCS-2030v2	Standard-Username ist “**root**” und das Passwort-Eingabefeld bleibt leer.
FCS-1060 / WCS-2060	Standard-Username ist “**root**” und das Passwort-Eingabefeld bleibt leer.
FCS-1081A	Standard-Username ist “**root**” und das Password ist **MAC address** (in Großbuchstaben).
FCS-1091 / WCS-1090	Standard-Username ist “**administrator**” und das Passwort-Eingabefeld bleibt leer.
FCS-1101	Standard-Username ist “**root**” und das Passwort ist **MAC address** (in Großbuchstaben).
FCS-0030 / WCS-0030	Standard-Username ist “**admin**” und das Passwort ist “**admin**”.

(MAC address wird auf dem Etikett des Gerätes angegeben.)

(Beispiel: 00116B73092E)

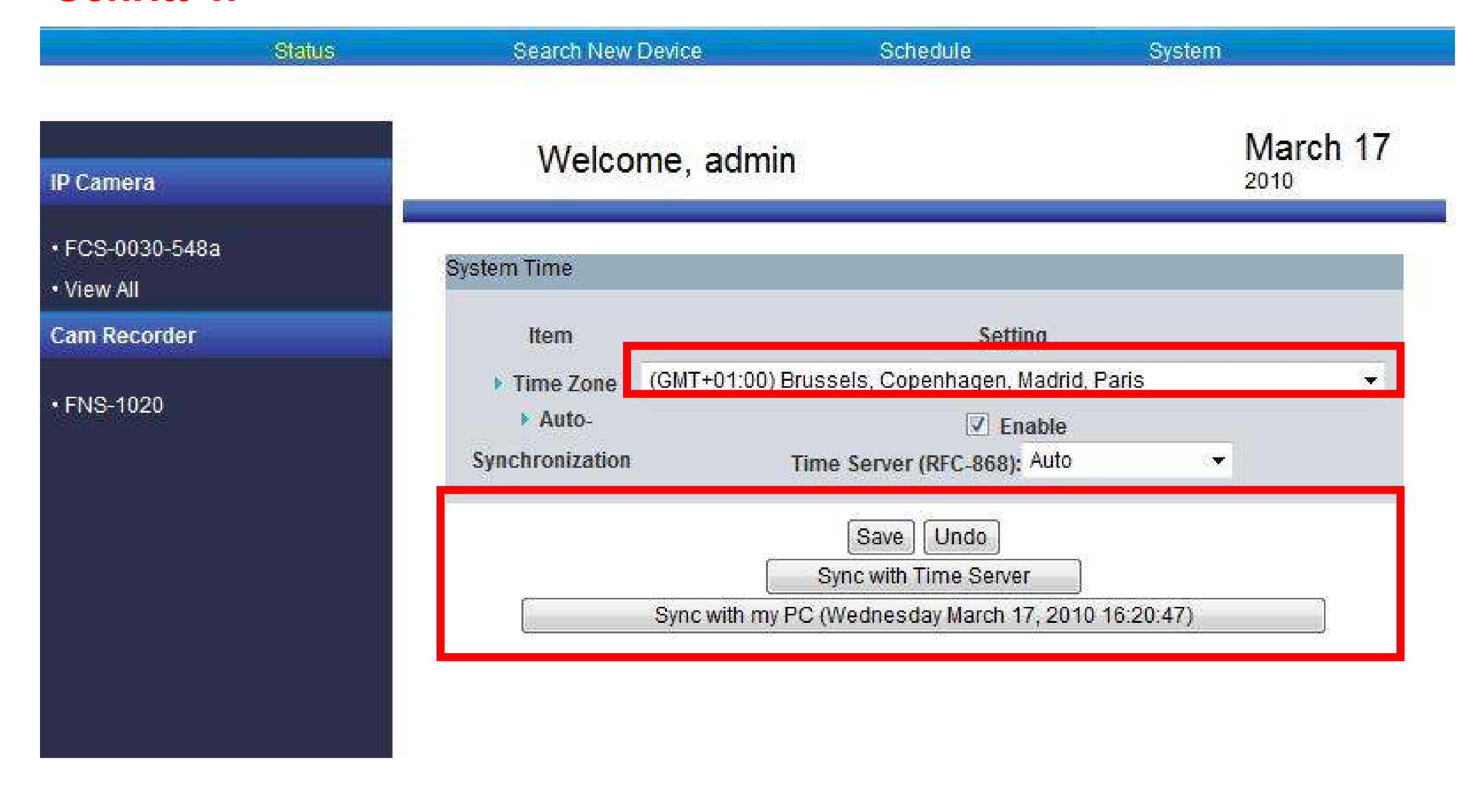
Schritt 3:



Bitte geben Sie “Username” und “Passwort” an.

Klicken Sie auf “Register”.

Schritt 4:



Synchronisation von Geräte- und Netzwerk-Zeit.

Klicken Sie auf "Save".

Schritt 5:

* FCS-0030-548a >>> Success
* WCS-0030-3355 >>> Success
* FNS-1020 >>> Success

Next

Klicken Sie auf "Next".

6.1.3 Einstellung der Geräte & Level1DNS

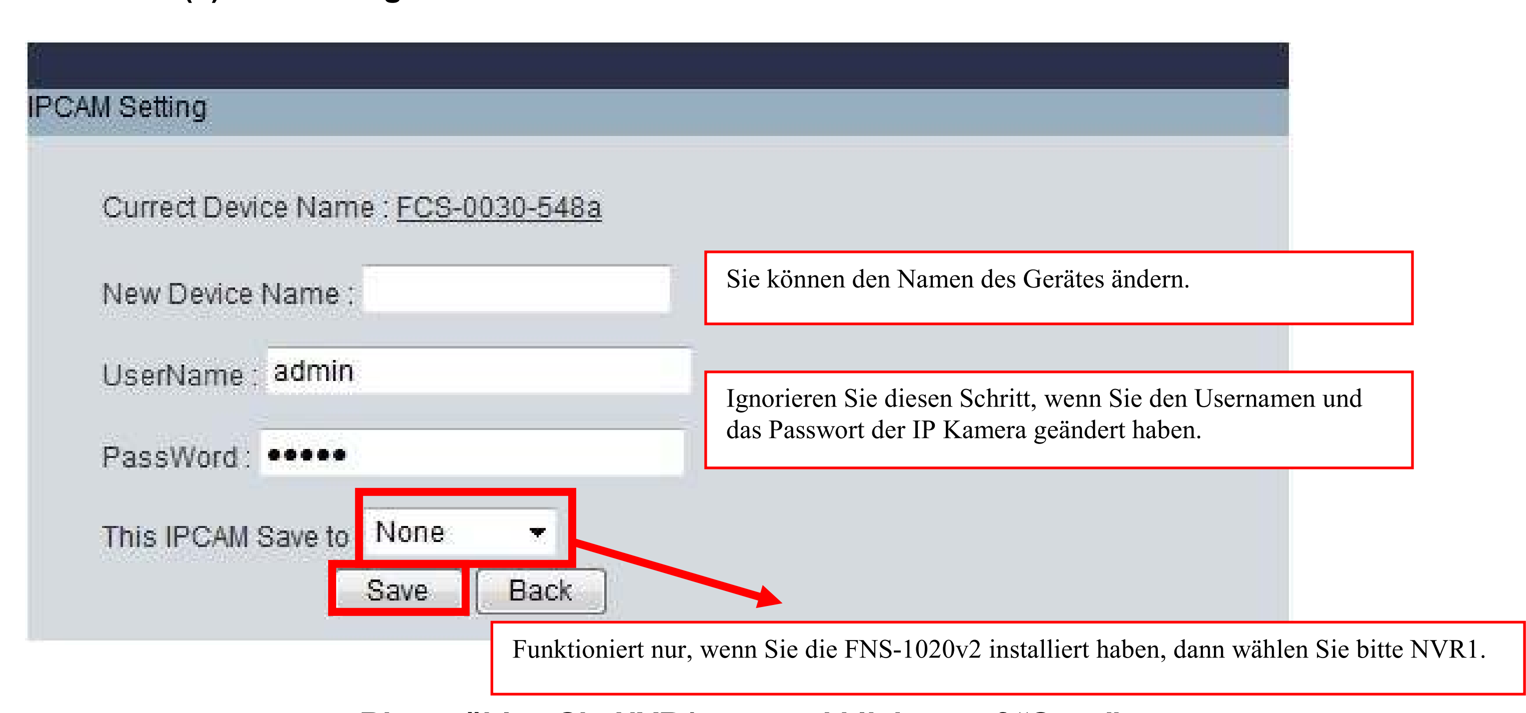
Einstellung des **Status** für Kamera & NVR.



Klicken Sie auf "Status".

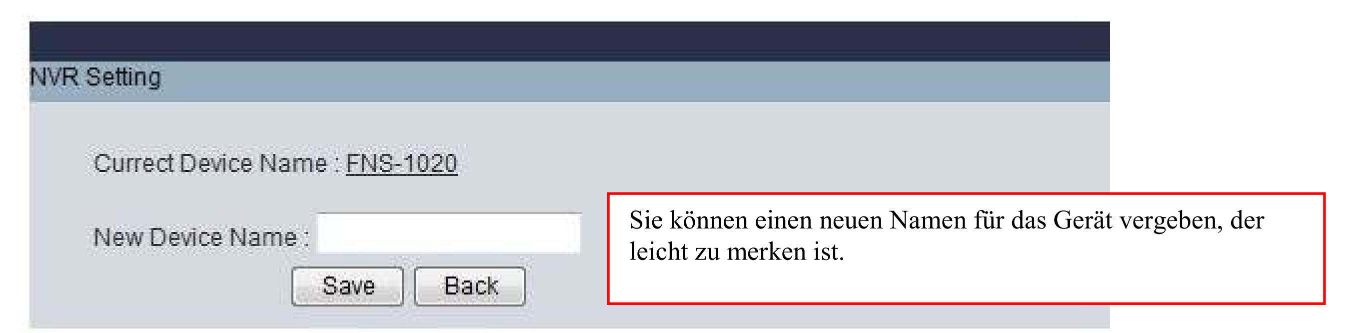
Das HomeGuard-System wird die registrierten IP-Kameras in einer Liste anzeigen. Diese können konfiguriert werden, indem die jeweilige Kamera angeklickt wird.
Sobald Sie die IP-Kamera(s) auf der Liste installiert haben, können Sie auf die jeweilige Kamera oder auf alle Kameras gleichzeitig per Live-Ansicht zugreifen.

IP Kamera(s) Einstellungen



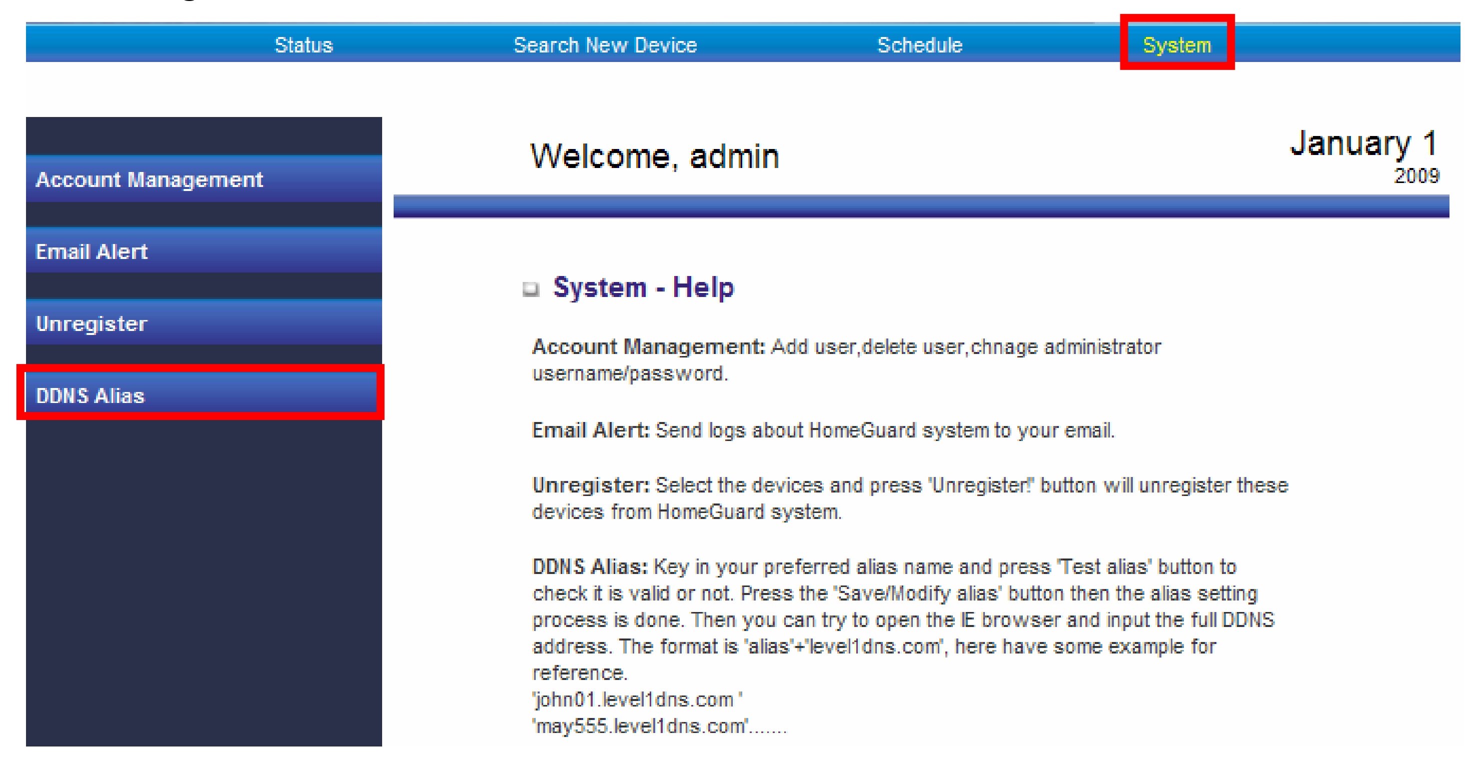
Bitte wählen Sie NVR1 aus und klicken auf "Save".

NVR Einstellungen



Sie können den Namen des Gerätes ändern oder dieses Feld frei lassen.
Klicken Sie auf **“Save”.**

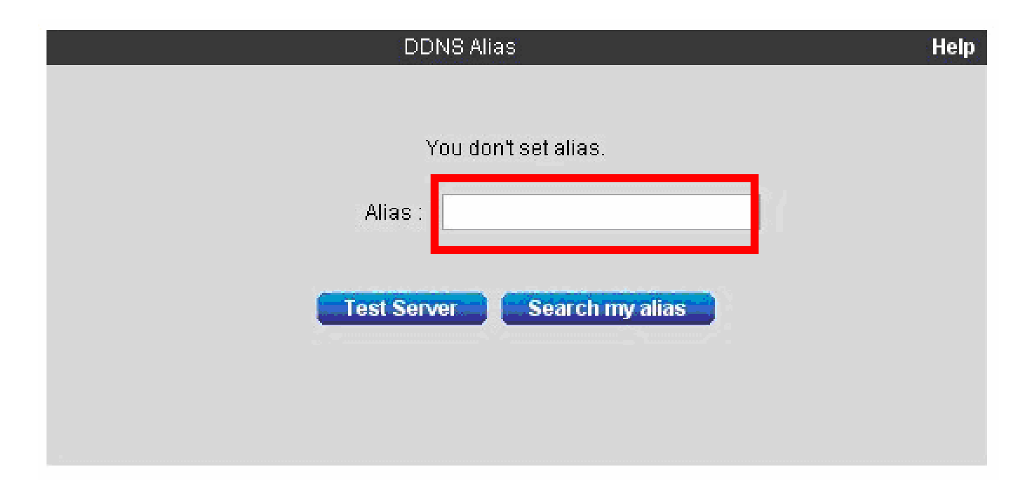
Einstellung des Level1DNS Domain-Namen



Klicken Sie auf “System” und dann auf “DDNS Alias”.

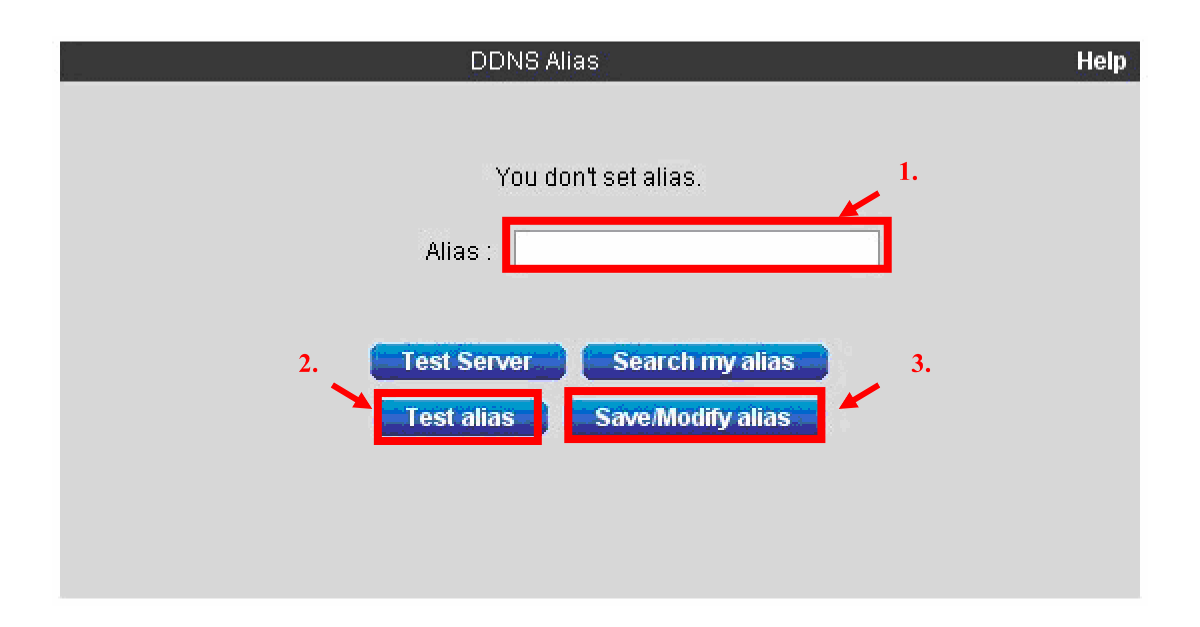
Sie können einen bevorzugten Alias-Namen erstellen und verwenden den neuen Level1DNS-Namen für den Internet-Zugriff überall dort wo Sie sich befinden.

Das Format ist “**Alias name or MAC address**”+”**level1dns.net**”.



Erstellen Sie einen Level1DNS Domain-Namen.

1. Geben Sie Ihren Alias-Namen ein → 2. Klicken Sie auf “Test alias” → 3. Sichern Sie per “Save/Modify alias”.



Bitte klicken Sie auf die Schaltflächen je nach Bedarf.

1. Klicken Sie auf **“Test Server”**, um zu testen, ob der Level1DNS.net Service verfügbar ist oder nicht.
2. Klicken Sie auf **“Search my alias”**, um die Suche nach Ihrem Alias-Namen zu starten.
3. Klicken Sie auf **“Test alias”**, um zu prüfen, ob der Alias-Name bereits vergeben ist oder nicht.
4. Klicken Sie auf **“Save/Modify alias”**, um die Einstellungen zu speichern.

Standardmäßig wird der Domain-Name durch MAC address (Beispiel: 00116B73092E) bestimmt. Nachdem Sie Ihren Alias-Namen erstellt haben, wird Ihr Domain-Name in "Ihren geänderten Namen".Level1DNS.net geändert (Beispiel: henry.level1DNS.net).
Sie können nun Videos von überall im IE-Browser anschauen, nachdem Sie **http:// "Ihr Name".level1DNS.net** eingeben haben.

6.2 Video-Ansicht

Schauen Sie sich das Video einer einzigen IP Kamera an.

Schritt 1:



Klicken Sie auf die IP Kamera Liste auf der linken Seite.

Schritt 2:

IP Camera
• FCS-0030-548a
• WCS-0030-3355
• View All
Cam Recorder
• FNS-1020
Welcome, admin
March 17
2010
FCS-0030-548a
Record Stop Snap
*Hard disk surplus capacity 36.84 GB

Wählen Sie die Kamera(s) zur Ansicht aus.

Schritt 3:

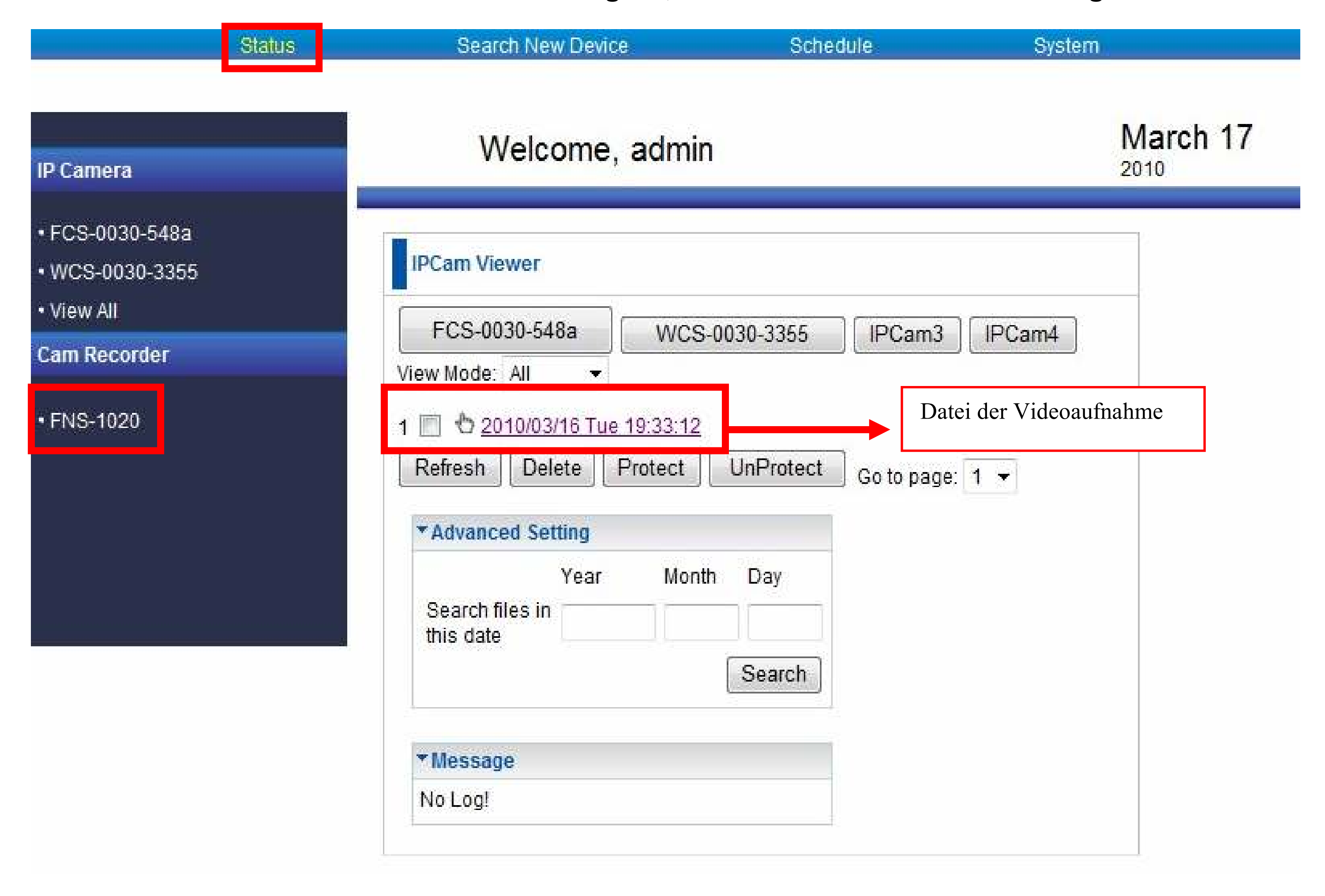


Klicken Sie auf “Record” und es wird eine 10-minütige Aufnahme auf dem FNS-1020 gespeichert.
Gehen Sie zum Menü “Schedule”, um einen Aufnahme-Zeitplan zu konfigurieren.

Wenn Sie keine Videoanzeige erhalten, nutzen Sie bitte den IE Bowser um “Active-X” zuerst zu installieren. Versuchen Sie es dann erneut.

6.2.1 Wiedergabe der Aufnahme

HInweis: Diese Funktion ist nur dann verfügbar, wenn Sie einen FNS-1020v2 registriert haben.



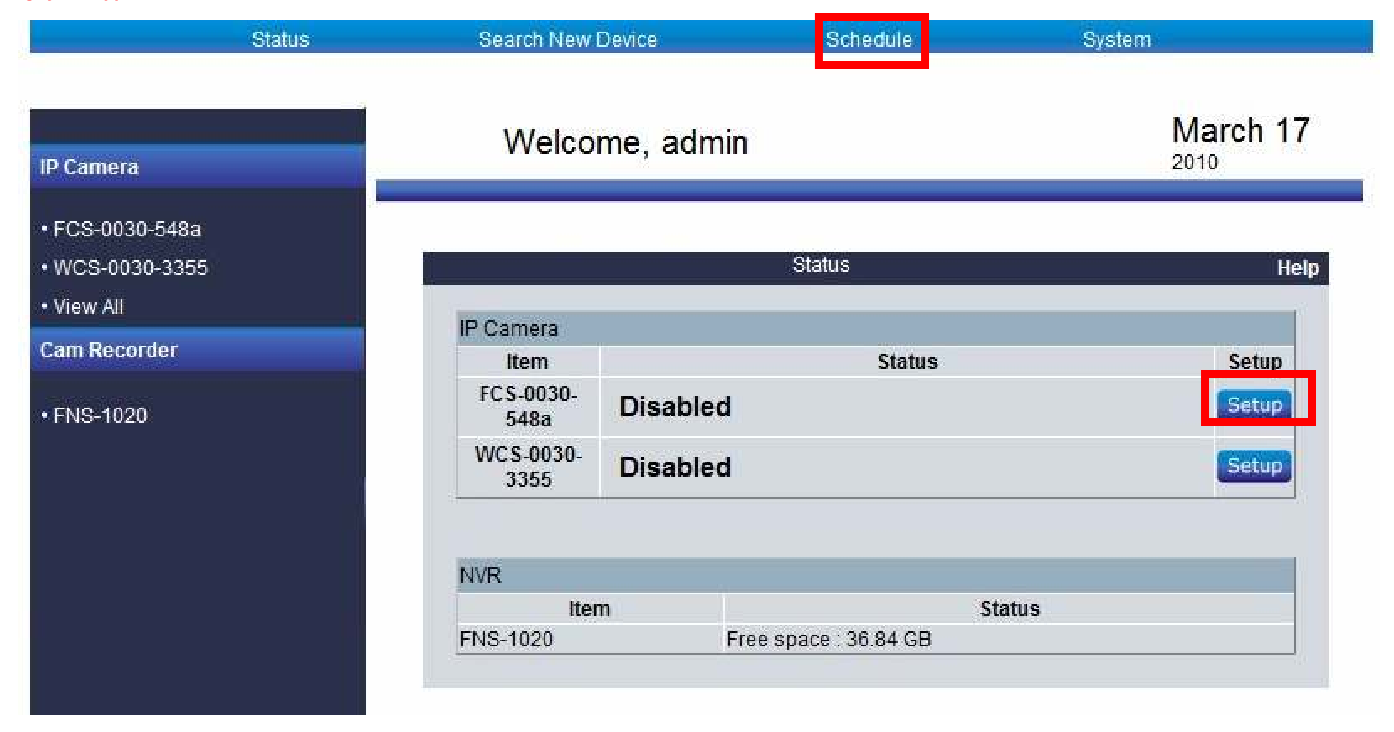
Klicken Sie auf “Status” und dann auf “FNS-1020.
Nutzen Sie den Rechten-Mausklick, um die aufgenommen Videodateien zu sichern und abzuspielen.

Wenn das Video nicht angezeigt wird, installieren Sie bitte den neuen Media Player/Codec, z.B. "VLC Media Player" oder "K-Lite Codec Pack" oder "KMPlayer", und versuchen Sie es dann erneut.

Hier ist ein Link zur Ihrer Information: http://www.videolan.org/vlc/

6.2.2 Zeitgesteuerte Aufnahme

Schritt 1:



Klicken Sie auf **"Schedule"** und dann **"Setup"**, um die Einstellungen des Zeitplanes vorzunehmen.

Schritt 2:

Status
Search New Device
Schedule
System
IP Camera
• FCS-0030-548a
• View All
Cam Recorder
• FNS-1020
Welcome, admin
March 17
2010
IPCam Schedul Rule
Schedul Rule Settings
Schedul Rule: Enable
Each file`s recording time length: 10 Minutes
Reserved disk space: 1 (GB)
When no enough space: Stop record Overwrite oldest file.
Select Schedul Type
Set date Set weekday Always
Save

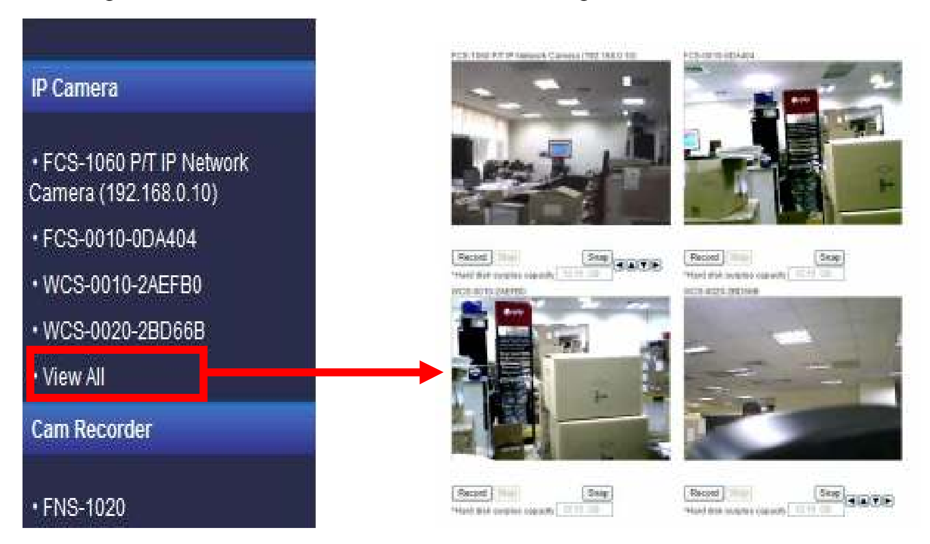
Klicken Sie auf "Save".

6.2.3 Anzeigen der IP-Kamera

6.2.3.1 Anzeigen sämtlicher IP-Kameras

Rufen Sie die Seite “View All” (Alles anzeigen) unter “Status” (Status), woraufhin hier Bilder von den richtig registrierten IP-Kameras angezeigt werden.

Nachtrag: Der WBR-6022 unterstützt eine Anzeige von bis zu 4 Kameras auf einer Weboberfläche.



6.2.3.2 Anzeigen einer IP-Kamera

Rufen Sie die Seite einer IP-Kamera unter “Status” (Status) auf, woraufhin das Bild der von Ihnen ausgewählten IP-Kamera hier angezeigt wird.



Der WBR-6022 unterstützt auch einige Schwenk-/Kippfunktionen von Kameras, wobei die Elemente für Schwenk-/Kippsteuerung nach Registrierung der Kamera angezeigt werden.



6.2.4Aufnehmen mit IP-Kamera

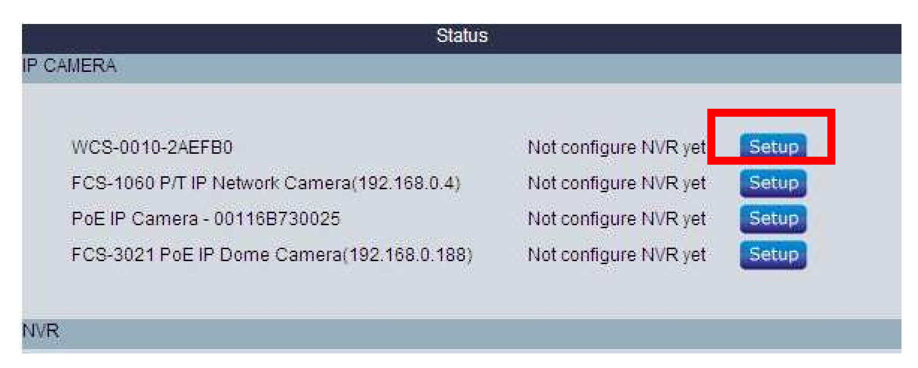
6.2.4.1 Einstellen des Aufnahmepfads

Sie MÜSSEN ein Speichergerät für das Abspeichern von Aufnahmedateien von jeder einzelnen IP-Kamera gewählt haben, bevor die Aufnahmefunktion aktiviert wird.

Klicken Sie in der "Status"-Hauptseite auf die Schaltfläche "Setup" (Einrichtung) der IP-Kamera, die Sie einrichten möchten, wobei Sie hier Ihrer IP-Kamera einen benutzerfreundlichen Namen geben und auch ggf. den Benutzernamen/das Kennwort ändern können. Zudem müssen Sie festlegen, auf welchem Netzwerkspeicher das Bild der IP-Kamera gespeichert werden soll.

Der Bildschirm sieht etwa folgendermaßen aus:

Klicken Sie auf das Symbol "SAVE" (Speichern), zeigt die Statusseite die Speicherinformationen jeder einzelnen IP-Kamera an.



6.2.4.2 Aufnehmen mit IP-Kamera

Bei angezeigten IP-Kameras können Sie durch Klicken auf die Schaltfläche “Record” (Aufnahme) Video von der IP-Kamera auf dem Netzwerkspeicher aufnehmen, bis Sie die Schaltfläche “Stop” (Stopp) anklicken.



6.2.4.3 Speichern von Bildschirmabbildern

Bei angezeigten IP-Kameras können Sie durch Klicken auf die Schaltfläche “Snap” (Einfangen) das derzeitige Bildschirmabbild aufzeichnen. Die Abbilddatei wird dann auf Ihrem PC gespeichert.



6.2.4.4 Programmieren der Aufnahmezeit

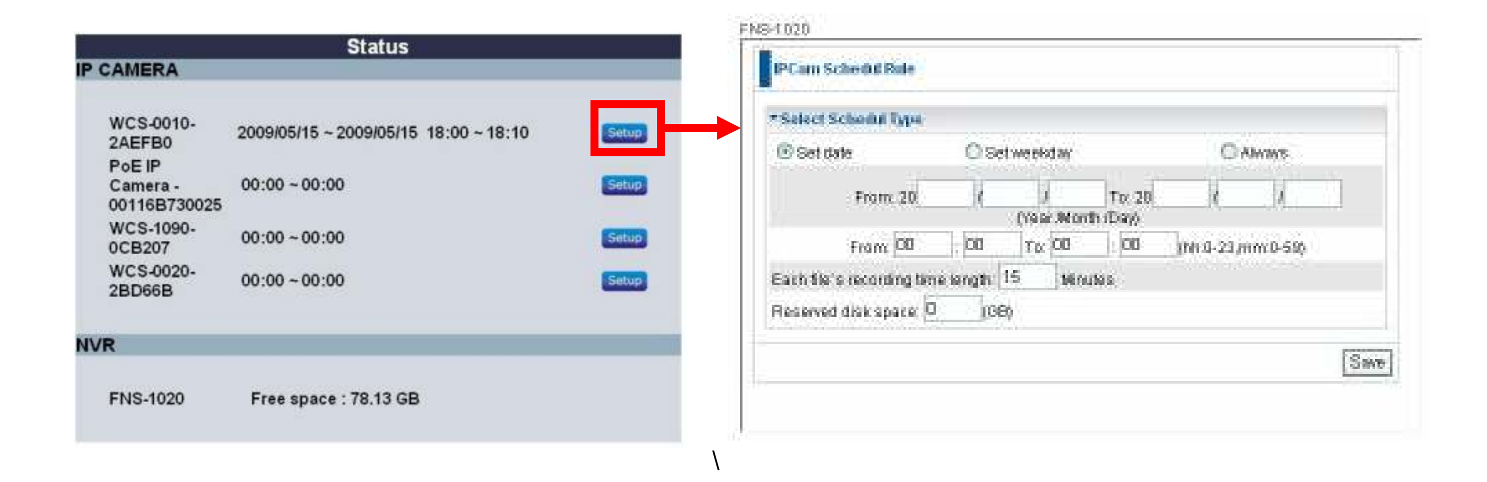
Mit diesem Gerät können Sie Ihre Zeitplanregeln für die Aufnahme von Video von der IP-Kamera einstellen.

Sie können den Zeitabschnitt einstellen und die IP-Kamera sowie den Netzwerkspeicher für den Speichervorgang angeben.

Zum Beispiel:

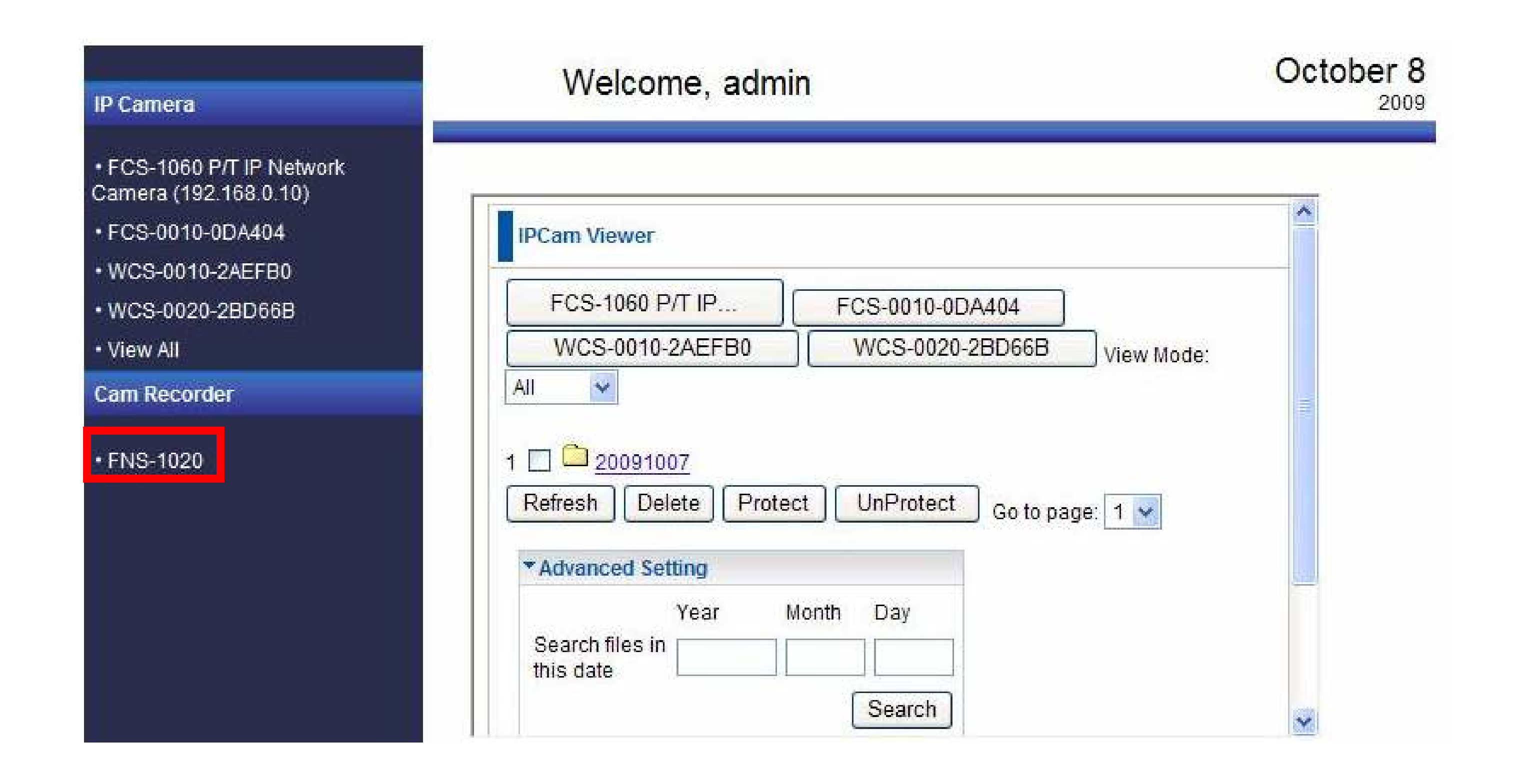
Jedesmal nehmen wir 15 Minuten von 8.30 Uhr bis 17.30 Uhr jeden Montag, Dienstag und Mittwoch auf.

Haben Sie die Option “Overwrite oldest file” (Älteste Datei überschreiben) gewählt, entfernt das HomeGuard-System die älteste Aufnahme aus dem Speicher, um die neue Aufnahme zu speichern, wenn der Speicherplatz kleiner ist als der von Ihnen eingerichtete Speicherplatz. Andernfalls stoppt der NVR (Network Video Recorder, Netzwerk-Videorekorder) die Aufnahme.



\

6.2.5Prüfen der Aufnahme auf dem FNS-1020 v2



Prüfen Sie den Datenspeicher

Nach Aufnahme von Video können Sie den Datenspeicher von der Weboberfläche aus überprüfen.

Rufen Sie die Seite “Storage” (Datenspeicher) auf; hier sind die Videodaten aufgelistet, nach Datum sortiert, mit jeder einzelnen IP-Kamera markiert.

Klicken Sie auf die Aufnahme, die Sie prüfen möchten und vom Netzwerkspeicher herunterladen können. Sie müssen den Media Player installieren, der das anzuzeigende Dateiformat unterstützt.

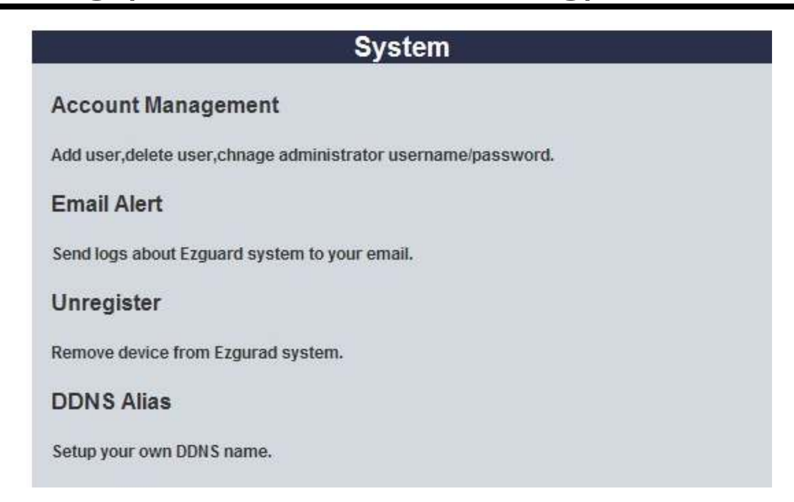
Löschen Sie die Aufnahme im Datenspeicher

Klicken Sie auf die Schaltfläche “Delete” (Löschen), wird die Aufnahme entfernt.

Schützen Sie die Aufnahme im Datenspeicher

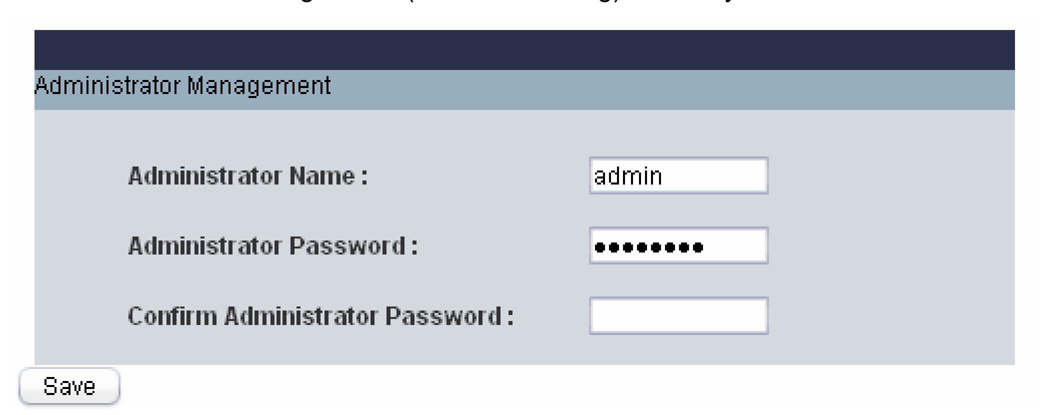
Klicken Sie auf die Schaltfläche “Protect” (Schützen), um zu verhindern, dass die Aufnahme gelöscht wird, wenn der Speicherplatz während einer programmierten Aufnahme nicht ausreichen sollte.

6.2.6Advanced Setting (Erweiterte Einstellung)



6.2.6.1 Account Management (Kontoverwaltung)

Klicken Sie auf den Link “Account Management” (Kontoverwaltung) unter “System”.



6.2.6.2 Administrator Management (Administratorverwaltung)

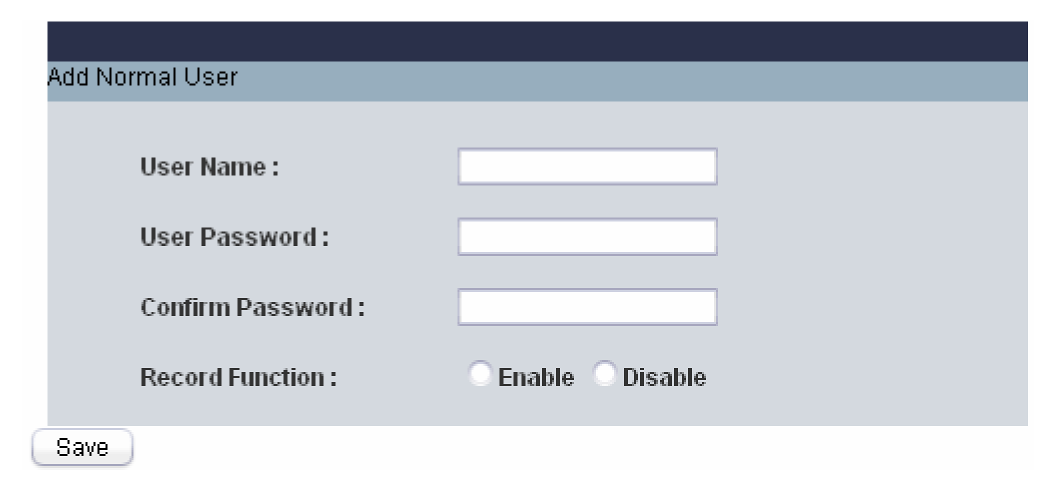
Hier können Sie den Benutzernamen/das Kennwort des Administratorkontos modifizieren.

Beachten Sie bitte, dass nur das Administratorkonto berechtigt ist, die Einstellung des HomeGuard-Systems zu modifizieren.

6.2.6.3 Add Normal User (Normalen Benutzer hinzufügen)

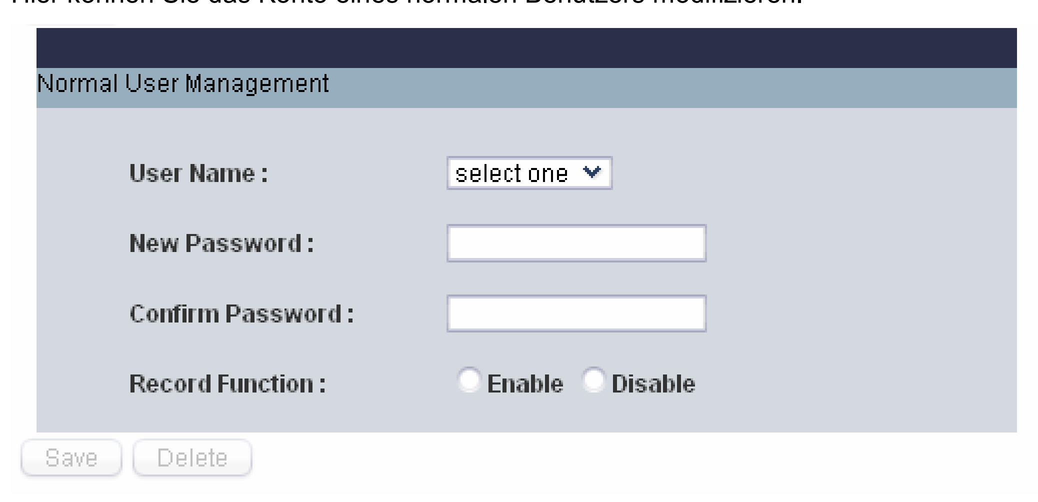
Hier können Sie das Konto eines neuen, normalen Benutzers hinzufügen.

Sie können für normale Benutzer festlegen, ob ihre Aufnahmefunktion aktiviert/deaktiviert sein soll.



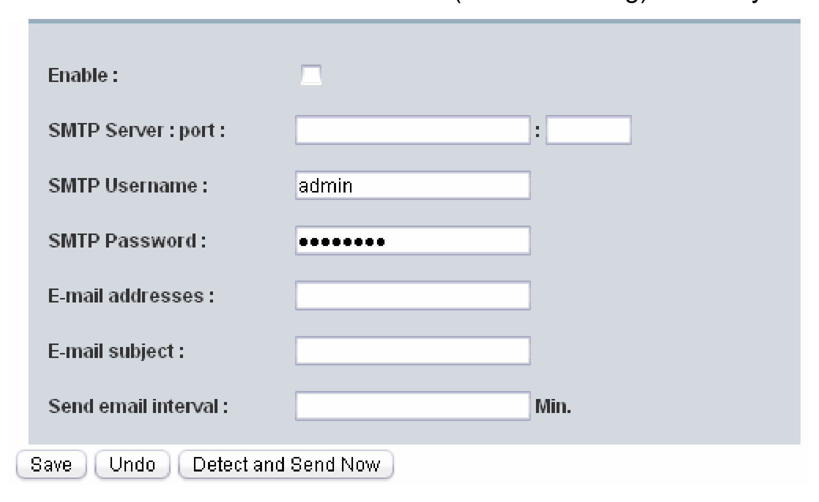
6.2.6.4 Normal User Management (Verwaltung des normalen Benutzers)

Hier können Sie das Konto eines normalen Benutzers modifizieren.



6.2.7Email Alert (E-Mailwarnung)

Klicken Sie auf den Link “Email Alert” (E-Mailwarnung) unter “System”, woraufhin sich folgender Bildschirm einblendet:



Geben Sie die Daten Ihrer E-Maileinstellung ein, um die E-Mailwarnfunktion zu aktivieren.

Das HomeGuard-System informiert Sie dann per E-Mail, wenn die Verbindung zu einem Systemgerät getrennt wurde.

6.2.8Unregister (Registrierung aufheben)

Klicken Sie auf den Link “Unregister” (Registrierung aufheben) unter “System”.



Wählen Sie Geräte aus und klicken Sie auf die Schaltfläche “Unregister!” (Registrierung aufheben), wird die Registrierung der betreffenden im HomeGuard-System aufgehoben.

6.2.9Ändern des Alias-Domänennamens

Klicken Sie auf den Link “DDNS Alias” (DDNS Alias) unter “System”.



DDNS Alias: Geben Sie Ihren bevorzugten Alias-Namen ein und drücken Sie die "Test alias"-Taste die Verfügbarkeit zu prüfen. Drücken Sie die "Save / Modify alias"-Taste um die Alias-Einstellung zu beenden. Dann können Sie versuchen, den Internet-Browser zu öffnen und geben Sie die vollständige DDNS-Adresse ein. Das Format ist "alias" + "level1dns.com", hier sind einige Beispiele:
“john01.level1dns.com “
“may555.level1dns.com”…….

Funktion der Tasten

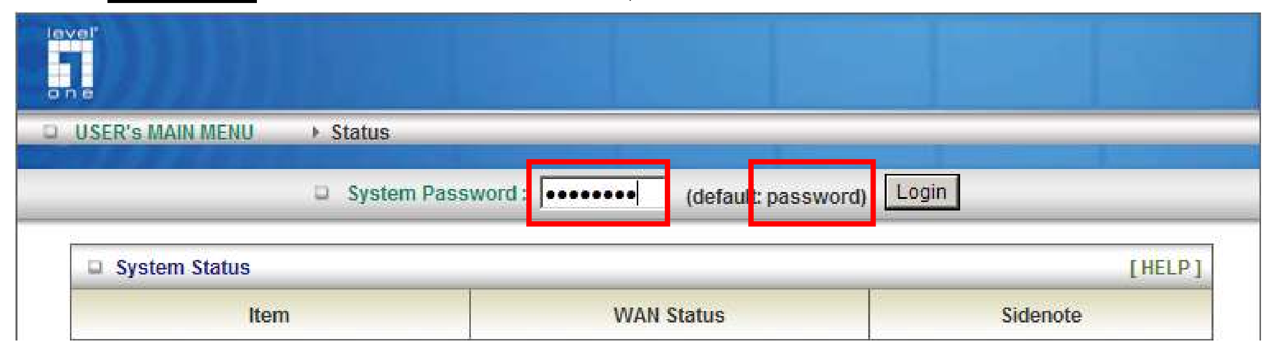
Test Server	Testen Sie, ob die Verbindung mit dem Level1DNS.net Service verfügbar ist oder nicht.
Search my alias	Suchen Sie Ihren Alias-Namen
Test alias	Sie können die Verfügbarkeit des Alias-Namen testen.
Save/Modify alias	Sichern der Einstellungen

Hinweis: Diese Einstellung muss sicherstellen, daß der HomeGuard WAN-Port mit einer öffentlichen IP arbeitet, damit die Funktion des DDNS zu 100% gewährleistet ist. Es darf keine Fehlbelegung geben (z.B. NAT, time out,…).

7 Router-Einstellung

Geben Sie “**password**” (ohne Anführungszeichen) in das Feld “Password” (Kennwort) ein und klicken Sie dann auf “Login” (Anmelden).

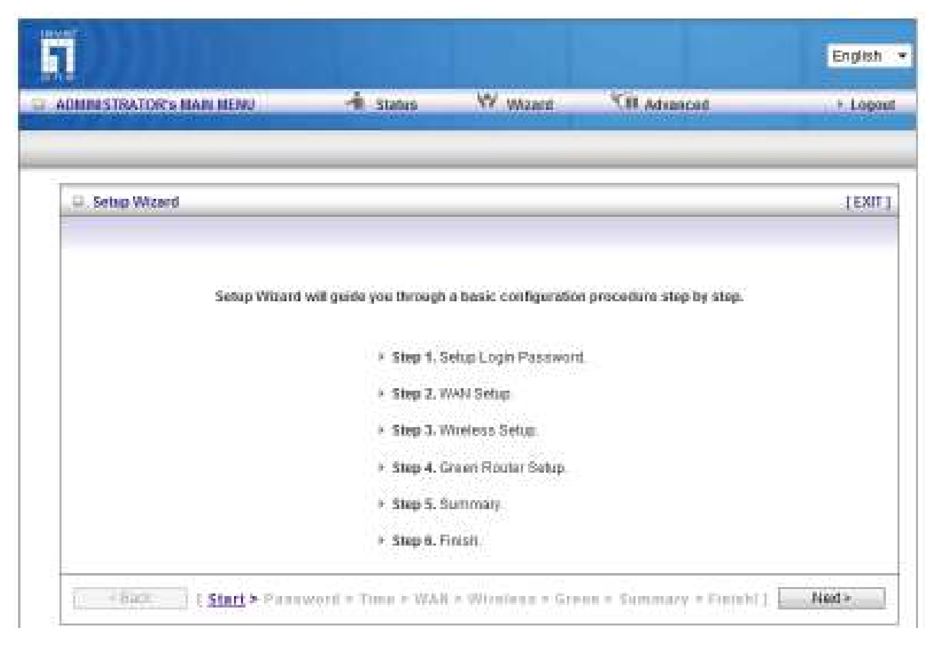
Hinweis: password ist das Standardkennwort, um sich bei dem Gerät anzumelden.



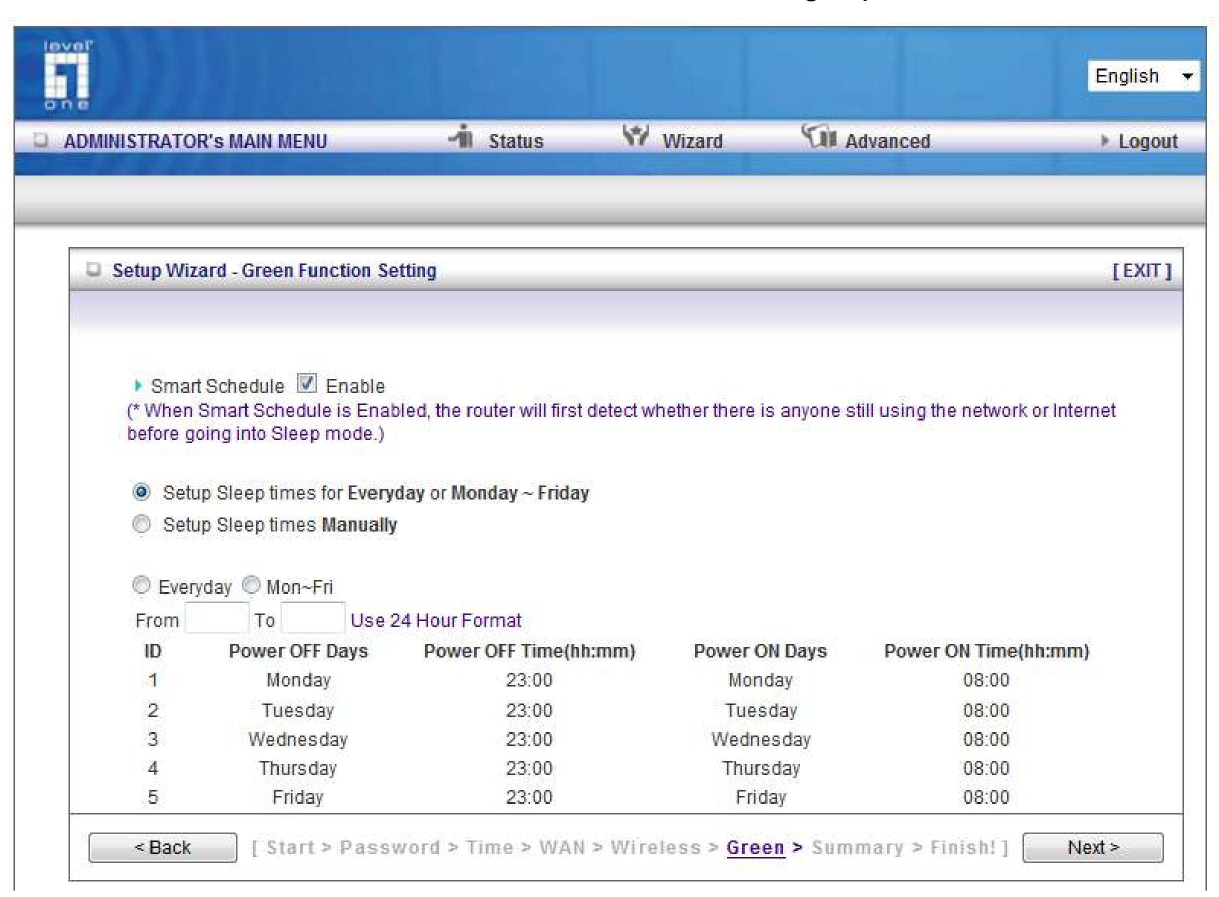
Der Benutzer kann die Verbindung mit Wizard (Assistent) schrittweise fertigstellen.
Wenn Sie ein erfahrener Benutzer sind, können Sie die Konfigurationen direkt unter Advanced Setup (Erweiterte Einrichtung) aufrufen.



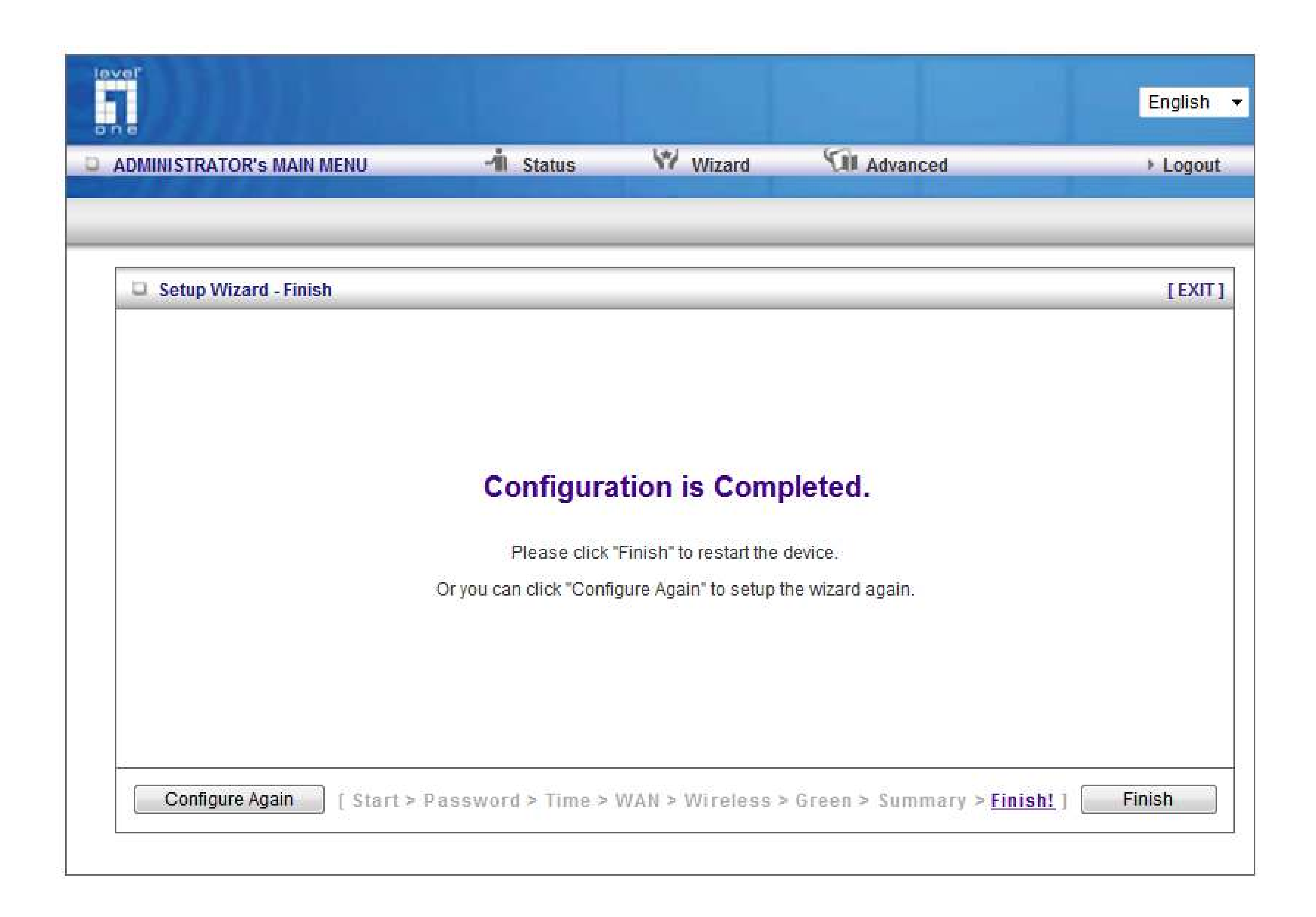
Der Setup Wizard (Einrichtungsassistent) führt Sie schrittweise durch eine grundlegende Konfiguration. Klicken Sie auf **Next (Weiter)**, um zu beginnen.



Vergessen Sie nicht, den Ruhemodus einzurichten, um die Energiesparfunktionen zu aktivieren.

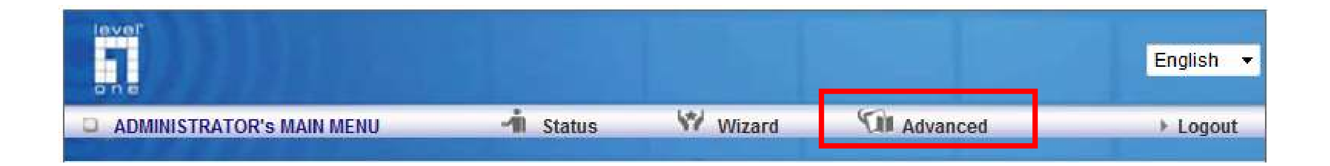


Sobald der Benutzer die entsprechenden Schritte fertiggestellt hat, wird der nachstehende Router-Bildschirm angezeigt. Dies bedeutet, dass die Internetverbindung jetzt aufgebaut ist.

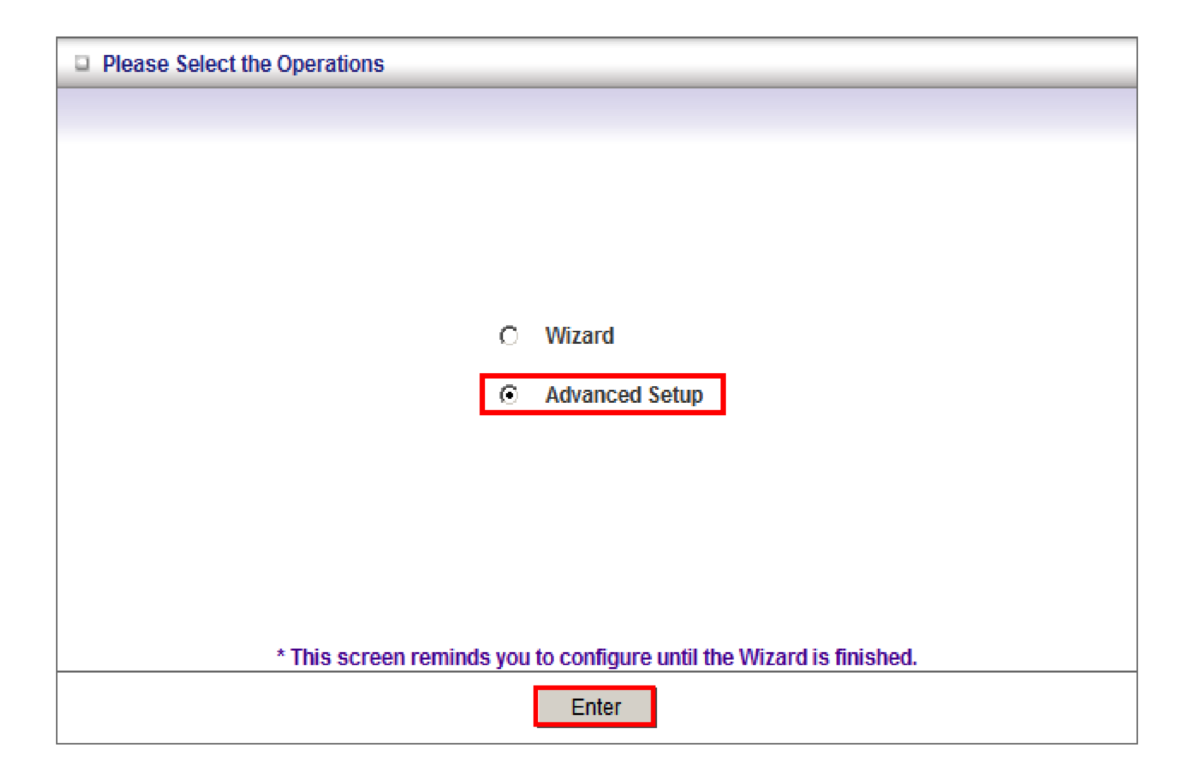

English
ADMINISTRATOR's MAIN MENU
Status
Wizard
Advanced
Logout
Setup Wizard - Finish
[EXIT]
Configuration is Completed.
Please click "Finish" to restart the device.
Or you can click "Configure Again" to setup the wizard again.
Configure Again
[Start > Password > Time > WAN > Wireless > Green > Summary > Finish!]
Finish

8 Advanced Setup (Erweiterte Einrichtung)

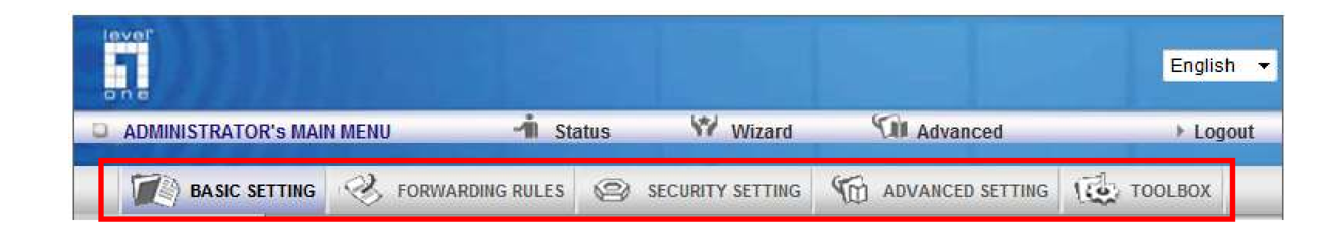
Um auf die erweiterte Einrichtung zuzugreifen, klicken Sie oben auf der Seite auf **Advanced Setup (Erweiterte Einrichtung)**.



Oder wählen Sie bei erstmaliger Installation den Punkt “Advanced Setup” (Erweiterte Einrichtung) und klicken Sie auf **Enter (Eingabe)**.

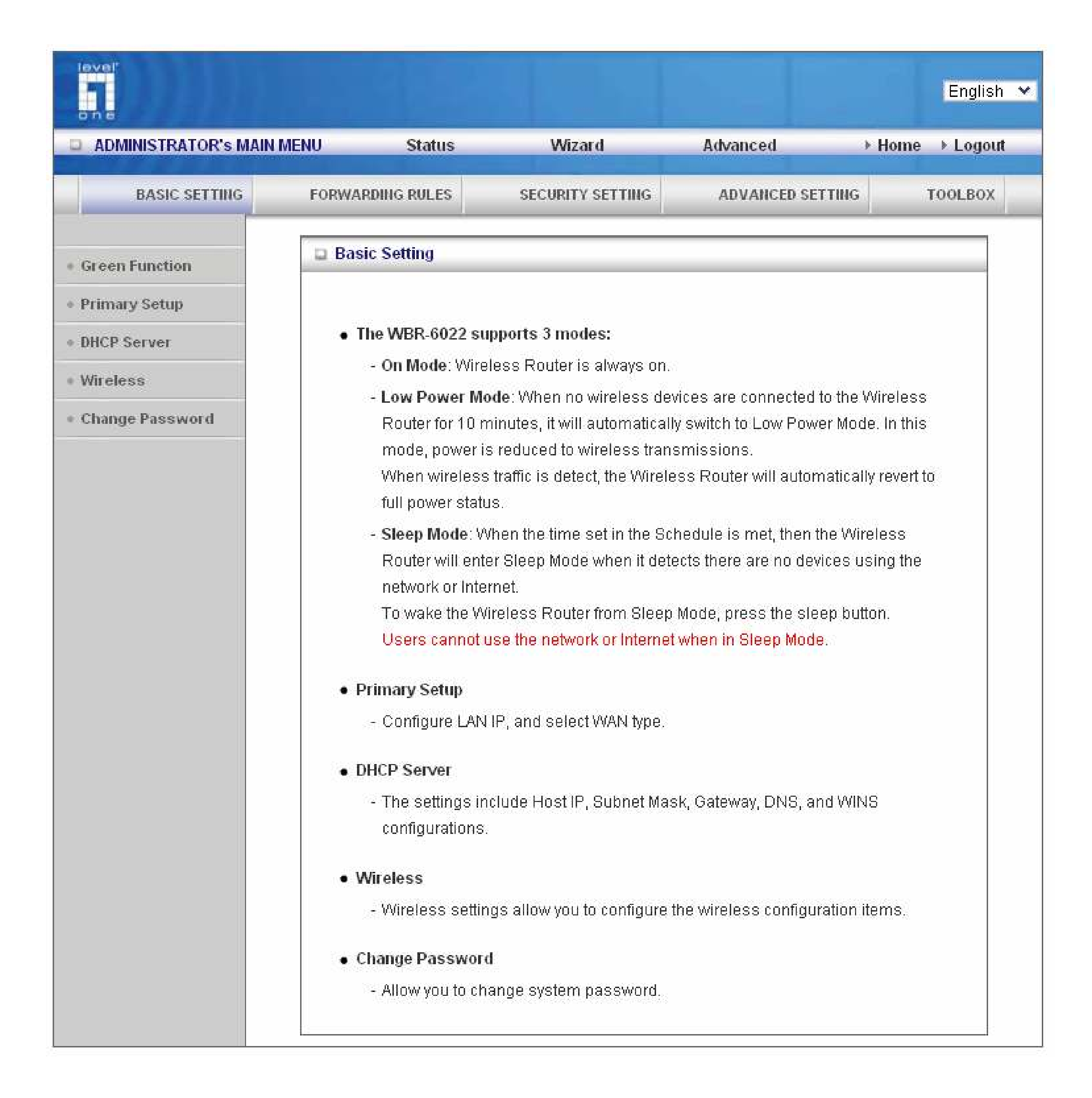


Gleich nach Aufruf von Advanced Setup (Erweiterte Einrichtung) sehen Sie folgendes Menü.



Basic Setting (Grundeinstellung)

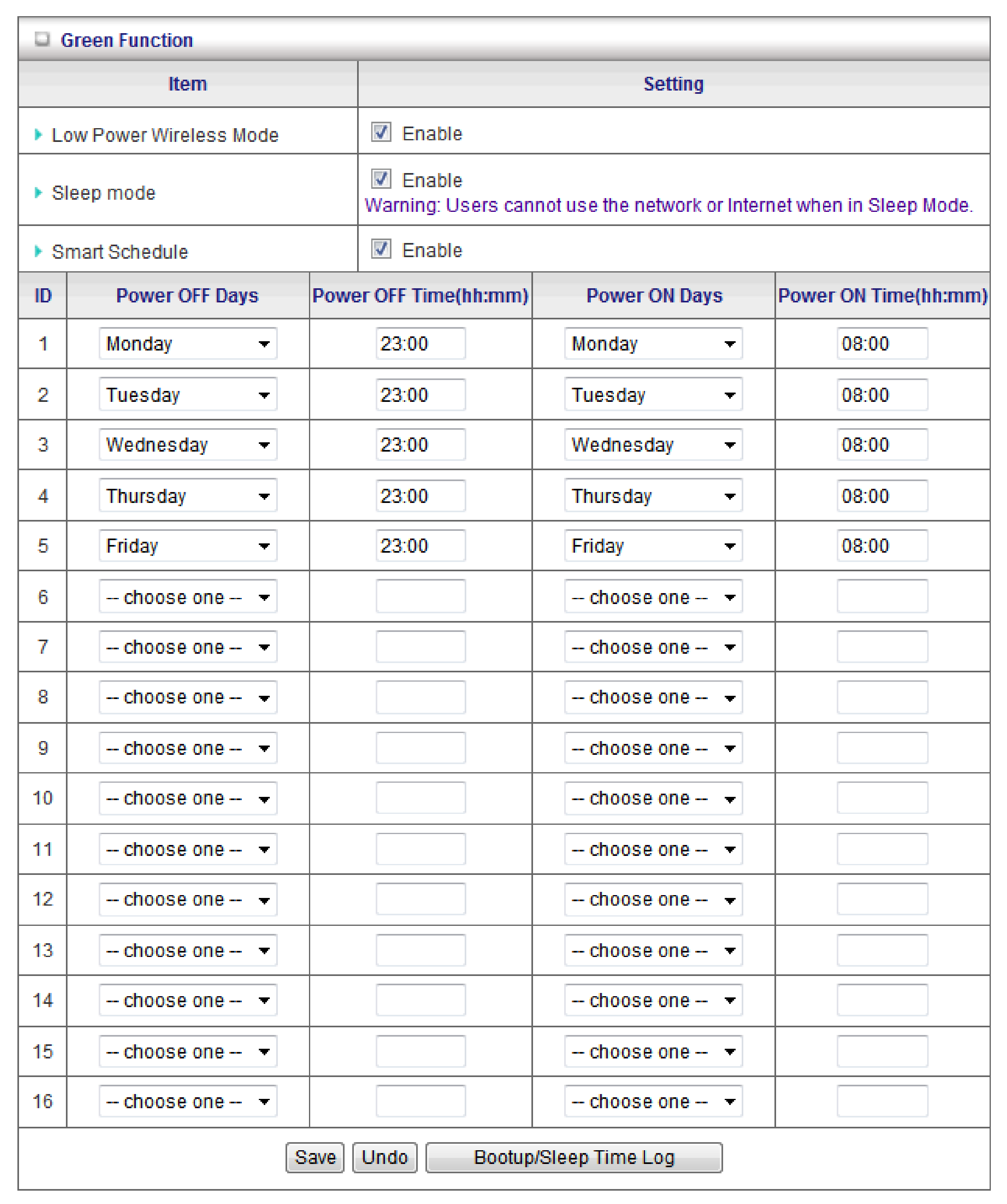
Es handelt sich hier um die Grundeinstellungen des Geräts. Klicken Sie in das Menü links, um die Seite mit den dazugehörigen Einstellungen anzuzeigen.



Green Function (“Grüne” Funktion)

Die Energiesparfunktion ermöglicht Ihnen die Einstellung des Zeitpunkts, an dem der Router in den Ruhemodus wechselt.

Dies bedeutet, dass der Router sich zu den vom Benutzer festgelegten Zeiten automatisch ein- und ausschalten kann.



Green Function

Item	Setting
Low Power Wireless Mode	☑ Enable
Sleep mode	☑ Enable Warning: Users cannot use the network or Internet when in Sleep Mode.
Smart Schedule	☑ Enable

ID	Power OFF Days	Power OFF Time(hh:mm)	Power ON Days	Power ON Time(hh:mm)
1	Monday	23:00	Monday	08:00
2	Tuesday	23:00	Tuesday	08:00
3	Wednesday	23:00	Wednesday	08:00
4	Thursday	23:00	Thursday	08:00
5	Friday	23:00	Friday	08:00
6	-- choose one --		-- choose one --	
7	-- choose one --		-- choose one --	
8	-- choose one --		-- choose one --	
9	-- choose one --		-- choose one --	
10	-- choose one --		-- choose one --	
11	-- choose one --		-- choose one --	
12	-- choose one --		-- choose one --	
13	-- choose one --		-- choose one --	
14	-- choose one --		-- choose one --	
15	-- choose one --		-- choose one --	
16	-- choose one --		-- choose one --	

Save | Undo | Bootup/Sleep Time Log

Low Power Wireless Mode (Wenig Energie im Drahtlosmodus): Sind keine drahtlosen Clients mit dem Router verbunden, reduziert er den Energieverbrauch auf Funkverbindung, um Energie zu sparen. Sobald sich ein Gerät mit dem Router drahtlos verbindet, läuft er sofort wieder mit normalem Energieverbrauch.

Sleep Mode (Ruhemodus): Ist dieser Punkt auf "Enabled" (Aktiviert) gesetzt, wechselt der Router gemäß der im nachfolgenden Zeitplan festgelegten Zeiten in den Ruhemodus oder aktiviert wieder den Normalmodus. Befindet sich der Router im Ruhemodus, kann sich der Benutzer weder mit dem lokalen Netzwerk noch mit dem Internet verbinden.

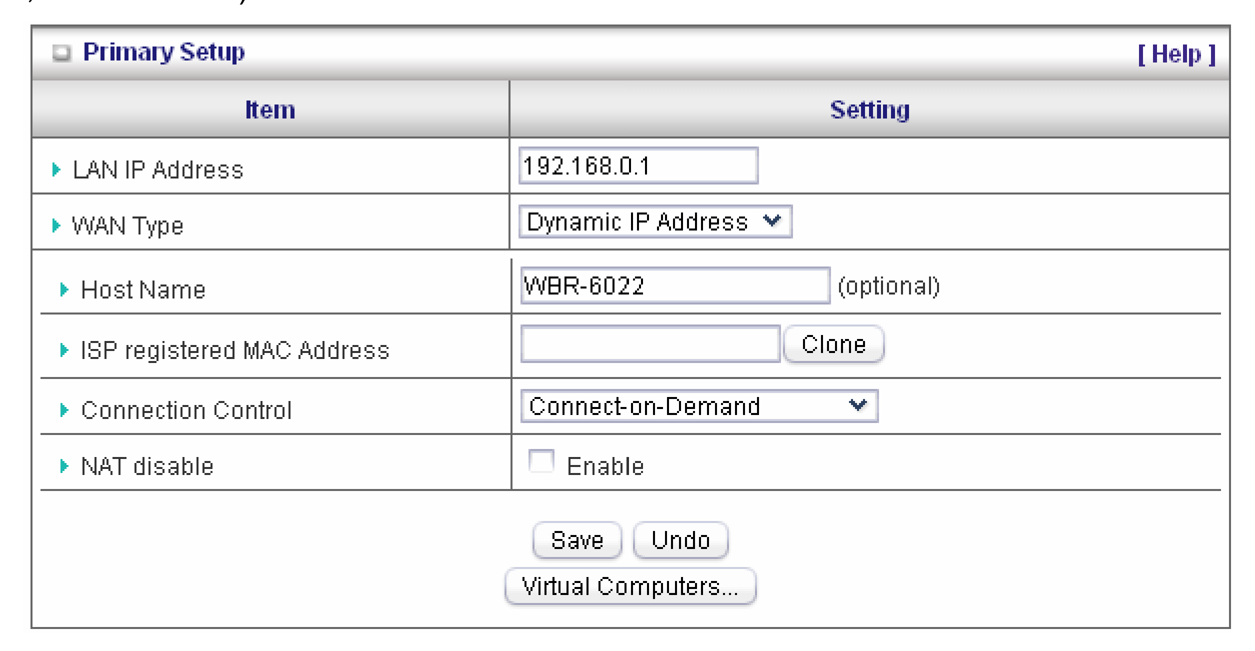
> **Hinweis:** Die Taste Sleep (Ruhezustand) auf der Rückseite des Router kann die derzeitige Router-Einstellung außer Kraft setzen. Sie können den Router zwingen, in den Ruhemodus zu wechseln oder wieder zum Normalmodus zurückzukehren.

Smart Schedule (Smarter Zeitplan): Ist dieser Punkt auf "Enable" (Aktivieren) gesetzt, prüft der Router erst, ob Aktivitäten im Netzwerk stattfinden, bevor der Router in den Ruhemodus wechselt. Dadurch wird verhindert, dass die Nutzung Ihres Netzwerks unterbrochen wird.

Bootup / Sleep Time Log (Systemstart-/Ruhezeitprotokoll): Ein Protokoll von den Zeiten, an denen der Router in den Ruhemodus wechselte oder wieder zum Normalmodus zurückkehrte.

Primary Setup (Primäre Einrichtung)

Auf dieser Seite können Sie die LAN-Einstellungen (Local Area Network, Lokales Netzwerk) auf Ihrem WBR-6022 *HomeGuard 22 Residential Gateway* und die WAN-Verbindung (Wide Area Network, Fernnetzwerk) ändern.



> **LAN IP Address (LAN-IP-Adresse):** Dies ist die lokale IP-Adresse dieses Geräts. Die Computer in Ihrem Netzwerk müssen die LAN-IP-Adresse Ihres Geräts als Standardgateway benutzen. Sie können sie bei Bedarf ändern.

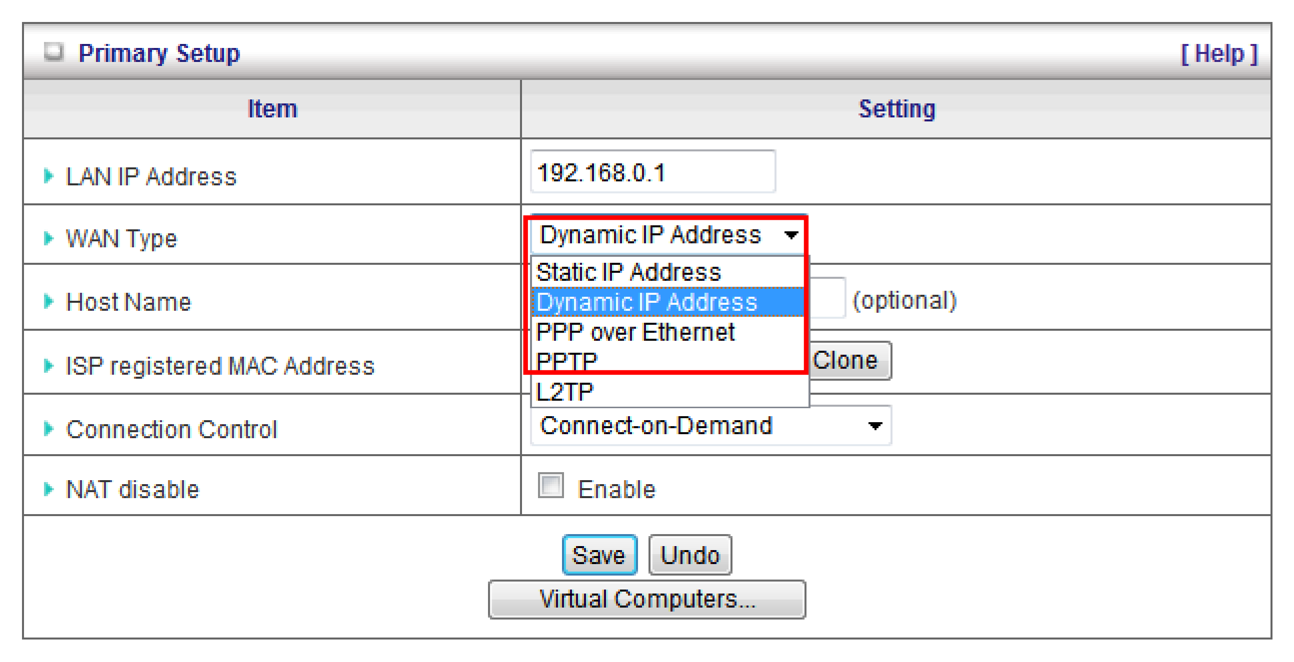
WAN Type (WAN-Typ): Dies ist der WAN-Verbindungstyp Ihres Internet-Dienstanbieters. Sie können im Listenmenü die für Sie geeignetste Option aus den folgenden Optionen auswählen:

Connection Control (Verbindungskontrolle): Hier können Sie die Methode auswählen, nach der der Router eine Verbindung mit dem Internet aufrechterhält.

Connect-on-Demand (Verbindung nach Bedarf): Der Router verbindet sich automatisch mit dem Internet, wenn ein Computer in dem Netzwerk eine Internetnutzung anfordert.

Auto-reconnect (always on) (Autom. neu verbinden (immer aktiviert)): Der Router hält die Verbindung zum Internet stets aufrecht, sofern möglich. Er verbindet auch automatisch neu, wenn er feststellt, dass er getrennt wurde.

Manually (Manuell): Sie müssen sich jedesmal manuell mit dem Internet verbinden.



Diese Option ermöglicht vorrangig, dass dieses Gerät richtig funktioniert. Die einstellbaren Punkte und die Webdarstellung hängen vom WAN-Typ ab. Wählen Sie den richtigen WAN-Typ, bevor Sie starten.

Static IP Address (Statische IP-Adresse): Die statische IP-Adresse wird Ihnen vom Internet-Dienstanbieter zugewiesen.

Dynamic IP Address (Dynamische IP-Adresse): Sie beziehen die IP-Adresse automatisch vom Internet-Dienstanbieter.

PPP over Ethernet (PPPoE, PPP über Ethernet): Bei einigen Internet-Dienstanbietern muss man sich mithilfe von PPPoE mit ihren Diensten verbinden.

PPTP (Point-to-Point Tunneling Protocol, Point-to-Point-Tunneling-Protokoll): Bei einigen Internet-Dienstanbietern muss man sich mithilfe von PPTP mit ihren Diensten verbinden.

L2TP (Layer 2 Tunneling Protocol, Layer 2 Tunneling-Protokoll): Bei einigen Internet-

Dienstanbietern muss man sich mithilfe von L2TP mit ihren Diensten verbinden.

Static IP Address (Statische IP-Adresse)

WAN-IP-Adresse, Subnetzmaske, Gateway, primäres und sekundäres DNS: Geben Sie die von Ihrem Internet-Dienstanbieter vorgegebenen Einstellungen ein.

Dynamic IP Address (Dynamische IP-Adresse)

1. Host Name (Hostname): Optional. Wird von einigen Internet-Dienstanbietern gefordert, z.B.: @Home.
2. Renew IP Forever (IP immer erneuern): Mit dieser Funktion ist Ihr Gerät in der Lage, Ihre IP-Adresse automatisch zu erneuern, wenn die Leasedauer abgelaufen ist—auch wenn das System inaktiv ist.

PPP over Ethernet (PPPoE, PPP über Ethernet)

1. PPPoE Account and Password (PPPoE-Konto und –Kennwort): Das von Ihrem Internet-Dienstanbieter zugewiesene Konto und Kennwort. Lassen Sie dieses Feld aus Sicherheitsgründen leer. Wenn Sie das Kennwort nicht ändern möchten, lassen Sie es leer.
2. PPPoE Service Name (PPPoE-Dienstname): Optional. Geben Sie den Dienstnamen ein, wenn Sie dazu von Ihrem Internet-Dienstanbieter aufgefordert werden. Andernfalls lassen Sie das Feld leer.
3. Maximum Idle Time (Maximale Leerlaufzeit): Der Zeitwert der Inaktivität, bevor Ihre PPPoE-Sitzung getrennt wird. Setzen Sie diesen Wert auf Null oder aktivieren Sie "Auto-reconnect" (Autom. neu verbinden), um diese Funktion zu deaktivieren.
4. Maximum Transmission Unit (MTU, Maximale Übertragungseinheit): Die meisten Internet-Dienstanbieter geben Benutzern einen MTU-Wert. Der gebräuchlichste MTU-Wert ist 1492.
5. Connection Control (Verbindungskontrolle): Hier stehen 3 Modi zur Auswahl:
6. Connect-on-Demand (Verbindung nach Bedarf): Das Gerät stellt einen Link zum Internet-Dienstanbieter her, wenn Clients ausgehende Pakete versenden.
7. Auto-Reconnect (always on) (Autom. neu verbinden (immer aktiviert)): Das Gerät stellt einen Link zum Internet-Dienstanbieter her, bis die Verbindung aufgebaut ist.
8. Manually (Manuell): Das Gerät stellt erst dann einen Link her, wenn die Schaltfläche "Connect" (Verbinden) auf der Statusseite angeklickt wird.

PPTP (Point-to-Point Tunneling Protocol, Point-to-Point-Tunneling-Protokoll)

Prüfen Sie zuerst, was Ihnen Ihr Internet-Dienstanbieter zugewiesen hat, und wählen Sie dann "Static IP Address (Statische IP-Adresse) oder "Dynamic IP Address" (Dynamische IP-Adresse).

1. My IP Address (Meine IP-Adresse) und My Subnet Mask (Meine Subnetzmaske): Die private IP-Adresse und Subnetzmaske, die Ihnen von Ihrem Internet-Dienstanbieter zugewiesen wurde.
2. Server IP Address (Server-IP-Adresse): Die IP-Adresse des PPTP-Servers.
3. PPTP Account and Password (PPTP-Konto und –Kennwort): Das von Ihrem Internet-Dienstanbieter zugewiesene Konto und Kennwort. Wenn Sie das Kennwort nicht ändern möchten, lassen Sie es leer.
4. Connection ID (Verbindungskennung): Optional. Geben Sie die Verbindungskennung ein, wenn Sie dazu von Ihrem Internet-Dienstanbieter aufgefordert werden.
5. Maximum Idle Time (Maximale Leerlaufzeit): Die Leerlaufzeit, nach derem Ablauf Ihre PPTP-Sitzung getrennt wird. Setzen Sie diesen Wert auf Null oder aktivieren Sie "Auto-Reconnect" (Autom. neu verbinden), um diese Funktion zu deaktivieren. Ist "Auto-Reconnect" (Autom. neu verbinden) aktiviert, verbindet sich dieses Gerät nach einem Neustart des Systems oder getrennter Verbindung automatisch mit dem Internet-Dienstanbieter.
6. Connection Control (Verbindungskontrolle): Hier stehen 3 Modi zur Auswahl:
7. Connect-on-Demand (Verbindung nach Bedarf): Das Gerät stellt einen Link zum Internet-Dienstanbieter her, wenn Clients ausgehende Pakete versenden.
8. Auto-Reconnect (always on) (Autom. neu verbinden (immer aktiviert)): Das Gerät stellt einen Link zum Internet-Dienstanbieter her, bis die Verbindung aufgebaut ist.
9. Manually (Manuell): Das Gerät stellt erst dann einen Link her, wenn die Schaltfläche "Connect" (Verbinden) auf der Statusseite angeklickt wird.

L2TP (Layer 2 Tunneling Protocol, Layer 2 Tunneling-Protokoll)

Prüfen Sie zuerst, was Ihnen Ihr Internet-Dienstanbieter zugewiesen hat, und wählen Sie dann “Static IP Address (Statische IP-Adresse) oder “Dynamic IP Address” (Dynamische IP-Adresse).

Zum Beispiel: Bei Verwendung der statischen IP-Adresse:

1. My IP Address (Meine IP-Adresse) und My Subnet Mask (Meine Subnetzmaske): Die private IP-Adresse und Subnetzmaske, die Ihnen von Ihrem Internet-Dienstanbieter zugewiesen wurde.
2. Server IP Address (Server-IP-Adresse): Die IP-Adresse des PPTP-Servers.
3. PPTP Account and Password (PPTP-Konto und –Kennwort): Das von Ihrem Internet-Dienstanbieter zugewiesene Konto und Kennwort. Wenn Sie das Kennwort nicht ändern möchten, lassen Sie es leer.
4. Connection ID (Verbindungskennung): Optional. Geben Sie die Verbindungskennung ein, wenn Sie dazu von Ihrem Internet-Dienstanbieter aufgefordert werden.
5. Maximum Idle Time (Maximale Leerlaufzeit): Die Leerlaufzeit, nach derem Ablauf Ihre PPTP-Sitzung getrennt wird. Setzen Sie diesen Wert auf Null oder aktivieren Sie “Auto-Reconnect” (Autom. neu verbinden), um diese Funktion zu deaktivieren. Ist “Auto-Reconnect” (Autom. neu verbinden) aktiviert, verbindet sich dieses Gerät nach einem Neustart des Systems oder getrennter Verbindung automatisch mit dem Internet-Dienstanbieter.
6. Connection Control (Verbindungskontrolle): Hier stehen 3 Modi zur Auswahl:
   - Connect-on-Demand (Verbindung nach Bedarf): Das Gerät stellt einen Link zum Internet-Dienstanbieter her, wenn Clients ausgehende Pakete versenden.
   - Auto-Reconnect (always on) (Autom. neu verbinden (immer aktiviert)): Das Gerät stellt einen Link zum Internet-Dienstanbieter her, bis die Verbindung aufgebaut ist.
   - Manually (Manuell): Das Gerät stellt erst dann einen Link her, wenn die Schaltfläche “Connect” (Verbinden) auf der Statusseite angeklickt wird.

Virtual Computers (Virtuelle Computer) (nur für WAN-Typ mit statischer und dynamischer IP-Adresse)

Dies wird verwendet, wenn WAN auf DHCP oder eine statische IP-Adresse gesetzt ist, wobei der Benutzer der LAN-IP-Adresse eine globale IP-Adresse zuweisen kann.

Virtual Computers [Help]

ID	Global IP	Local IP	Enable
1			
2			
3			
4			
5			

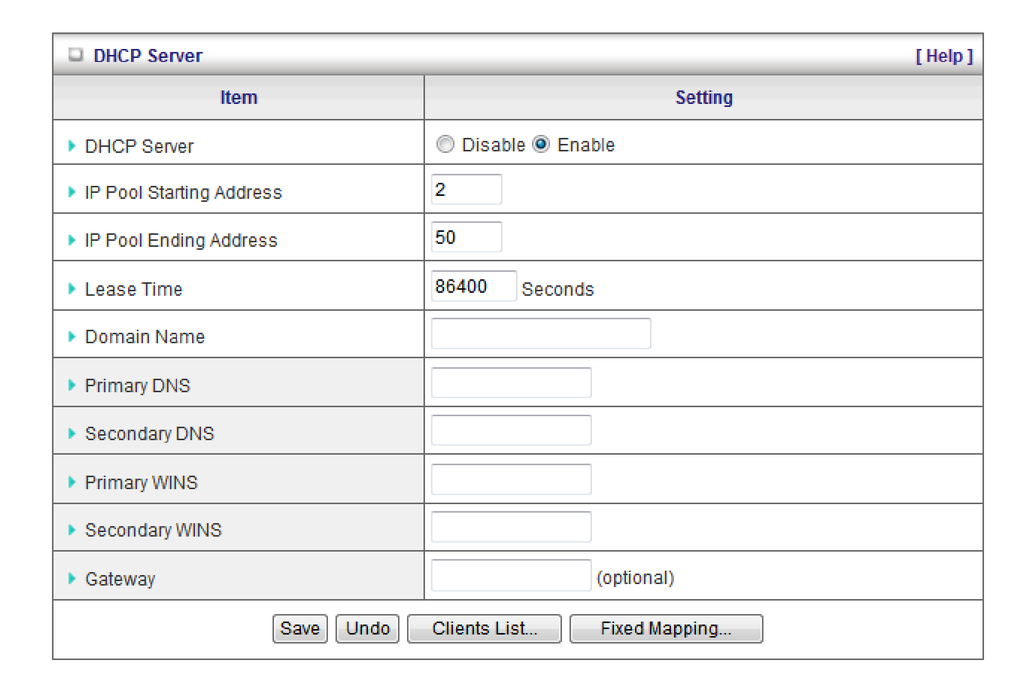
Save Undo Back

Mit Virtual Computer (Virtueller Computer) können Sie die originale NAT-Funktion aktivieren und können eine 1:1-Zuordnung der multiplen globalen IP-Adresse und der lokalen IP-Adresse einrichten.

- **Global IP (Globales IP):** Geben Sie die von Ihrem Internet-Dienstanbieter zugewiesene globale IP-Adresse ein.
- **Local IP (Lokales IP):** Geben Sie die lokale IP-Adresse Ihres LAN-PCs entsprechend der globalen IP-Adresse ein.
- **Enable (Aktivieren):** Versehen Sie dieses Kästchen mit einem Häkchen, um die Funktion “Virtual Computer” (Virtueller Computer) zu aktivieren.

DHCP Server (DHCP-Server)

Auf dieser Seite können Sie den DHCP-Server auf dem Router konfigurieren.



Weitere Einstellungen werden angezeigt, wenn Sie auf **More (Mehr)** klicken.

DHCP Server (DHCP-Server): Hier können Sie den DHCP-Server auf “Disable” (Deaktivieren) oder “Enable” (Aktivieren) setzen.

IP Pool Starting Address (IP-Pool-Startadresse)/IP Pool Ending Address (IP-Pool-Endadresse): Die IP-Pools, die Clients zugeordnet werden können.

Lease Time (Leasezeit): Die DHCP-Leasezeit für den DHCP-Client.

Domain Name (Domänenname): Hier können Sie einen Domänennamen (optional) zuweisen.

Primary DNS (Primäres DNS) / Secondary DNS (Sekundäres DNS): Hier können Sie DNS-Server (optional) zuweisen.

Primary WINS (Primäres WINS) / Secondary DNS (Sekundäres WINS): Hier können Sie WINS-Server (optional) zuweisen.

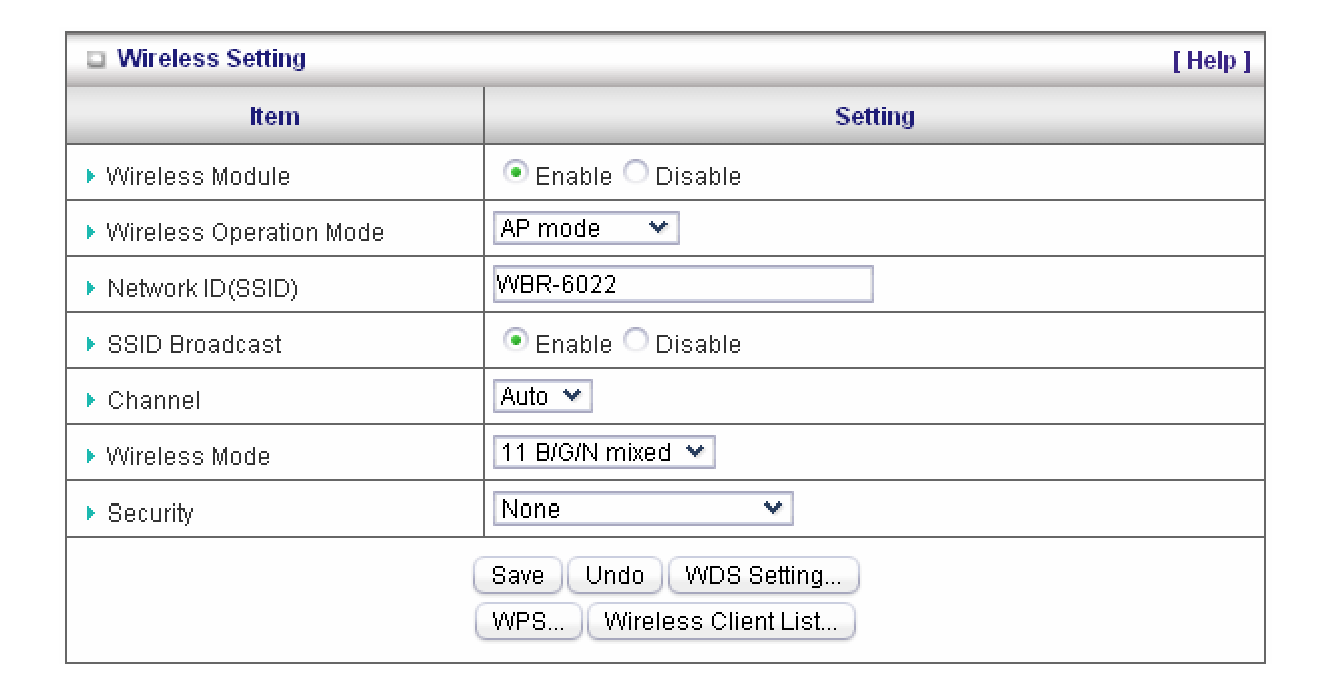
Gateway (Gateway): Die IP-Adresse eines alternativen Gateways (optional).

Clients List (Client-Liste): Prüft dieDHCP-Client-Liste.

Fixed Mapping (Feststehende Zuordnung): Bringt Sie zur Seite Security (Sicherheit) > MAC Control (MAC-Steuerung).

Nachdem Sie Ihre Auswahl getroffen haben, klicken Sie entweder auf **Save (Speichern)**, um die Einstellungen zu speichern, oder auf **Undo (Rückgängig)**, um den Vorgang zu beenden.

Wireless Setting (Drahtloseinstellung)



Wireless (Drahtlos) – Enabled (Aktiviert) per Standard. Bei Deaktivierung wird die Drahtlosfunktion dieses Geräts ausgeschaltet.

Wireless Operation Mode (Drahtloser Betriebsmodus): Hier haben Sie die Wahl zwischen Access Point (AP, Zugangspunkt) oder Wireless Client (Drahtlos-Client).

Hinweis: Der Modus Wireless Client (Drahtlos-Client) unterstützt die folgenden drahtlosen Verschlüsselungen: WEP, WPA-PSK (TKIP), WPA2-PSK (AES)

Network ID (SSID) (Netzwerkkennung): Die SSID (Service Set Identifier, Funknetzkennung) ist der Name, der einem bestimmten WLAN (Wireless Local Area Network, Lokales Drahtlosnetzwerk) gegeben wird. Die werkseitig eingestellte SSID lautet **WBR-6022**. Die SSID kann auf einfache Weise geändert werden, um ein neues Drahtlosnetzwerk aufzubauen.

Hinweis: SSID-Kennungen können aus bis zu 32 ASCII-Zeichen bestehen.

SSID Broadcast (SSID-Aussendung): Der WBR-6022 sendet Signale mit der SSID und anderen Drahtlosinformationen aus, so dass Computer oder andere Drahtlosgeräte den WBR-6022 bei der

Suche nach Drahtlosnetzwerken finden können. Deaktivieren Sie diese Funktion, wenn Sie Ihr Drahtlosnetzwerk ausblenden möchten.

Channel (Kanal): Die Nummer des Funkkanals. Die zugelassenen Kanäle hängen von der behördlichen Domäne ab. Die Standardeinstellung ist AUTO (Automatisch), wobei der WBR-6022 den am wenigsten verwendeten Kanal findet, um Störungen zu vermeiden.

Hinweis: Der Kanalbereich hängt von Ihren regionalen Bestimmungen ab. Beachten Sie hierzu die Kanaldetails in den technischen Daten.

Wireless Client List (Drahtlos-Client-Liste): Mit dieser Funktion können Sie die Geräte feststellen, die mit dem WBR-6022 über das Drahtlosnetzwerk verbunden sind.

Security (Sicherheit): Sicherheit – Sie können aus drei Verschlüsselungsstufen auswählen, um Ihr Drahtlosnetzwerk zu sichern:

No Encryption (Keine Verschlüsselung), WEP, 802.1x RADIUS, WPA-PSK, WPA, WPA2-PSK (AES), WPA2 (AES), WPA-PSK / WPA2-PSK und WPA1 / WPA2.

LevelOne empfiehlt **WPA2-PSK (AES)** für eine einfache und sichere Drahtlosverschlüsselung.

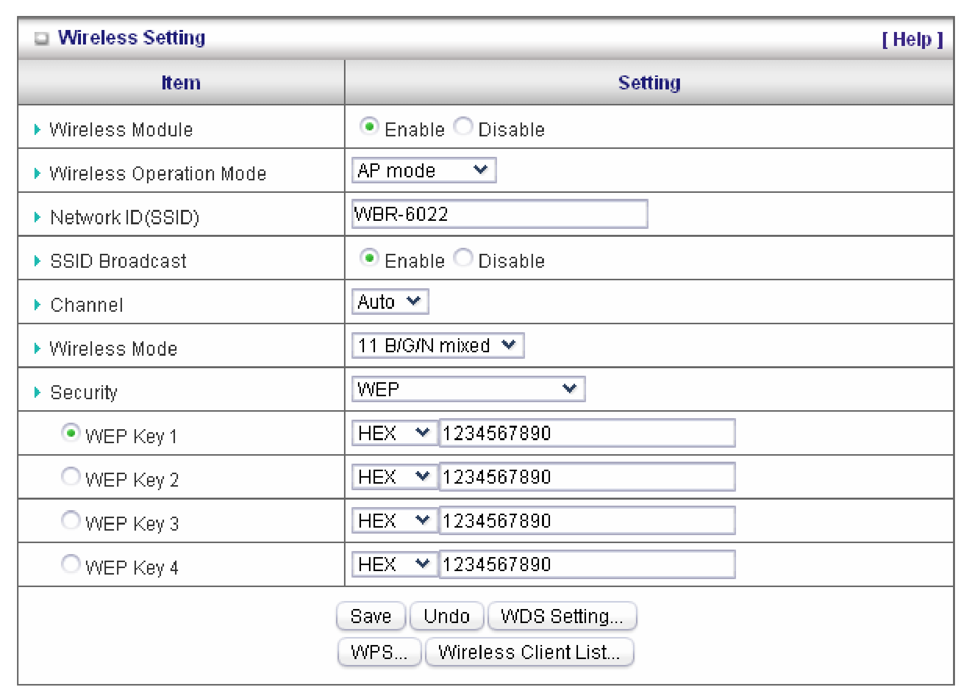
Nachdem Sie die drahtlosen Sicherheitseinstellungen auf dem WBR-6022 konfiguriert haben, müssen Sie dieselben Einstellungen auch auf Ihrem Drahtlosadapter konfigurieren, bevor Sie eine Drahtlosverbindung aufbauen können.

Beachten Sie bitte, dass nicht alle Adapter die verfügbaren Sicherheitsfunktionen unterstützen.

No Encryption (Keine Verschlüsselung) ist die Standardeinstellung (wie im obigen Bildschirm zu sehen ist).

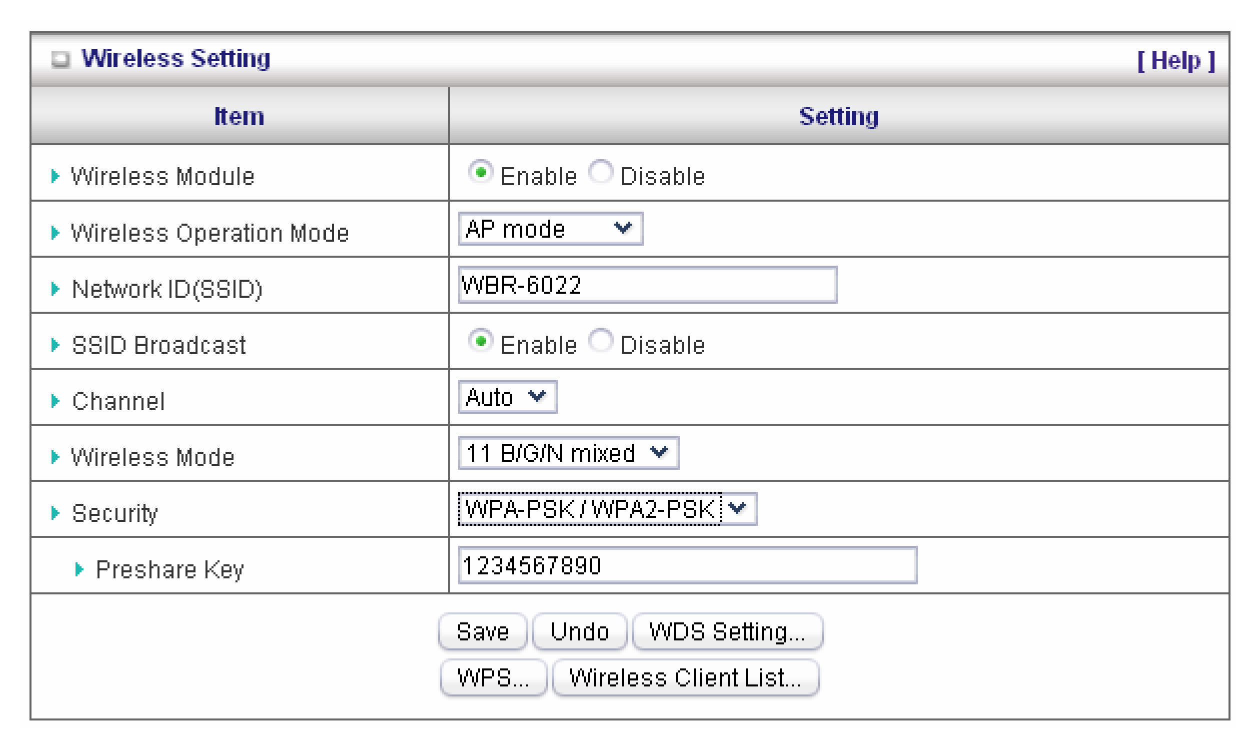
WEP (Wired Equivalent Privacy, Datenschutz ähnlich einer Drahtverbindung):

WEP (Wired Equivalent Privacy). Bei aktivierter Sicherheit werden Ihre Daten während der Übertragung zum WBR-6022 geschützt. Geben Sie den 10-stelligen WEP-Schlüssel ein.



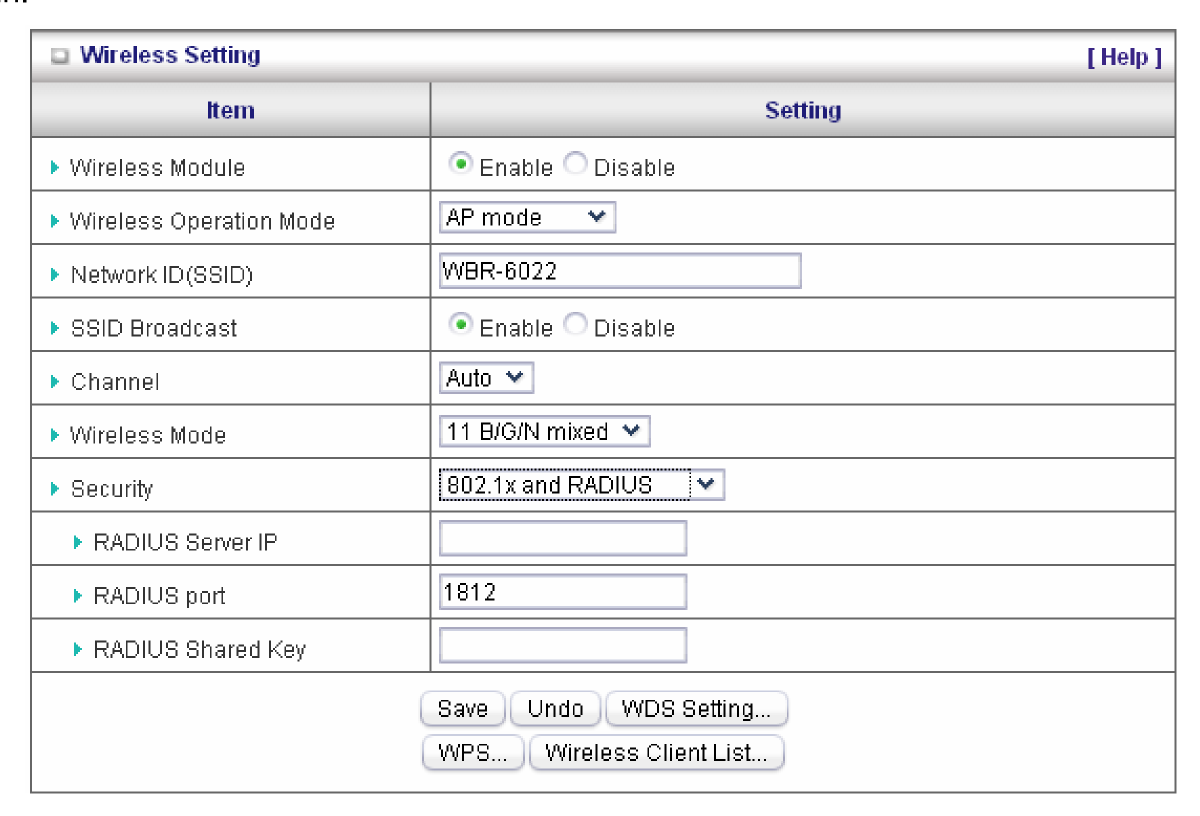
WPA-PSK, WPA2-PSK, WPA/WPA2-PSK

Diese Art von Sicherheit ist sicherer als WEP. Geben Sie den Schlüssel in das Feld “Preshare Key” (Vorinstallierter Schlüssel) ein. Das Feld kann 8 bis 63 Zeichen aufnehmen, die aus einer Kombination aus Buchstaben und Zahlen bestehen können.



802.1x und RADIUS

Zur Verwendung dieser Sicherheitsfunktion ist ein RADIUS-Server in Ihrem Netzwerk erforderlich, um den Zugang zu authentifizieren. Geben Sie die Details Ihres RADIUS-Servers ein.



RADIUS Server (RADIUS-Server)

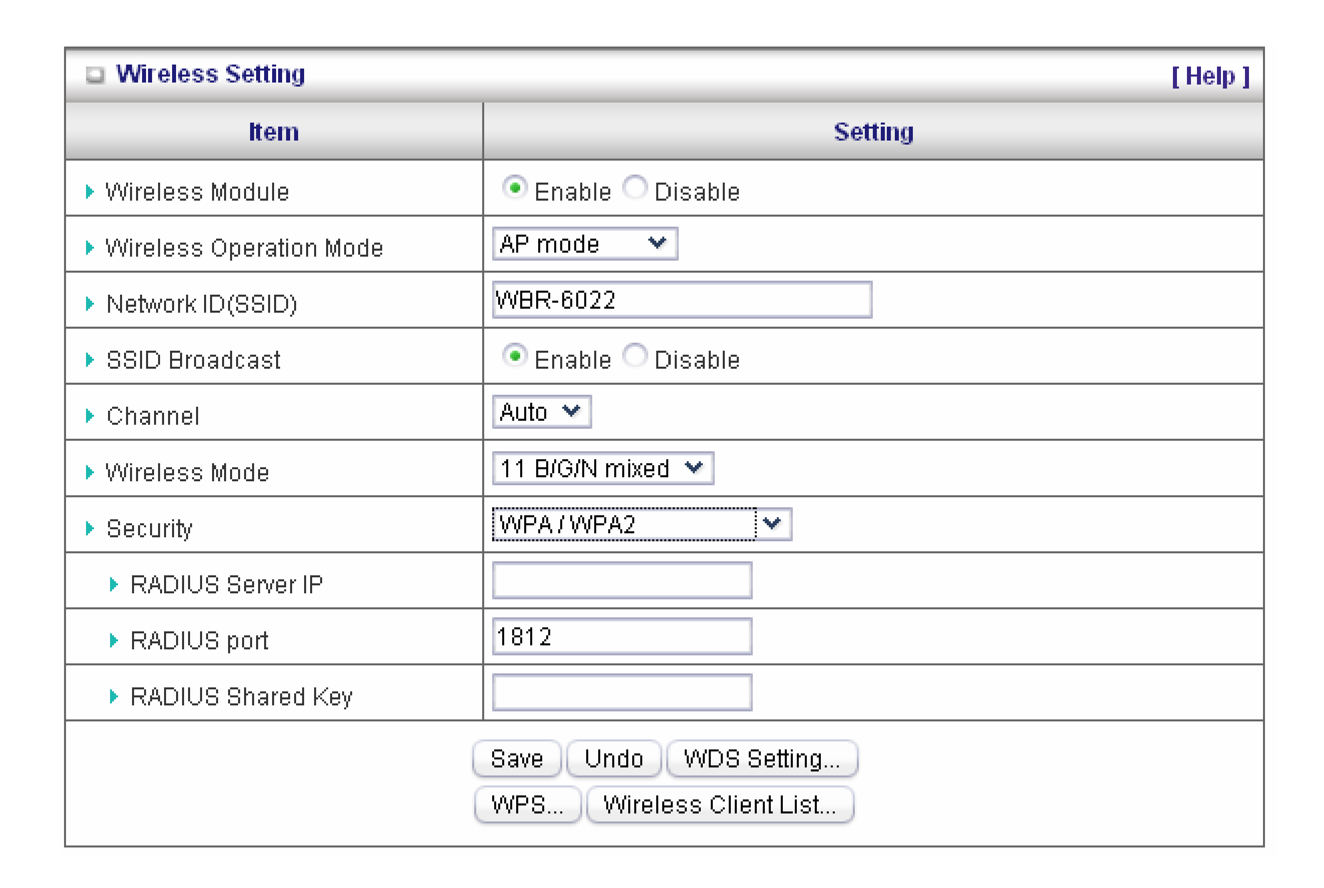
IP-Adresse oder der Domänenname des RADIUS-Servers.

RADIUS Shared Key (Freigegebener RADIUS-Schlüssel)

Schlüsselwert, der vom RADIUS-Server und diesem Router gemeinsam verwendet wird. Dieser Schlüsselwert stimmt mit dem Schlüsselwert im RADIUS-Server überein.

WPA, WPA2, WPA1/WPA2

Ähnelt der 802.1X-Sicherheit mit WPA / WPA2 für Verschlüsselung. Sie benötigen einen RADIUS-Server für Authentifizierung. Geben Sie die Details Ihres RADIUS-Servers ein.



RADIUS Server (RADIUS-Server)

- IP-Adresse oder der Domänenname des RADIUS-Servers.
- Port-Nummer des RADIUS-Servers.
- Geben Sie den “RADIUS Shared Key” (Freigegebener RADIUS-Schlüssel) ein Schlüsselwert, der vom RADIUS-Server und diesem Router gemeinsam verwendet wird. Dieser Schlüsselwert stimmt mit dem Schlüsselwert im RADIUS-Server überein.

WPS (WiFi Protected Setup, WiFi-geschützte Einrichtung)

Die WPS-Funktion folgt dem Wi-Fi Alliance WPS-Standard und erleichtert die Einrichtung von Wi-Fi-Netzwerken mit aktivierter Sicherheit in Klein- und Heimbüros.

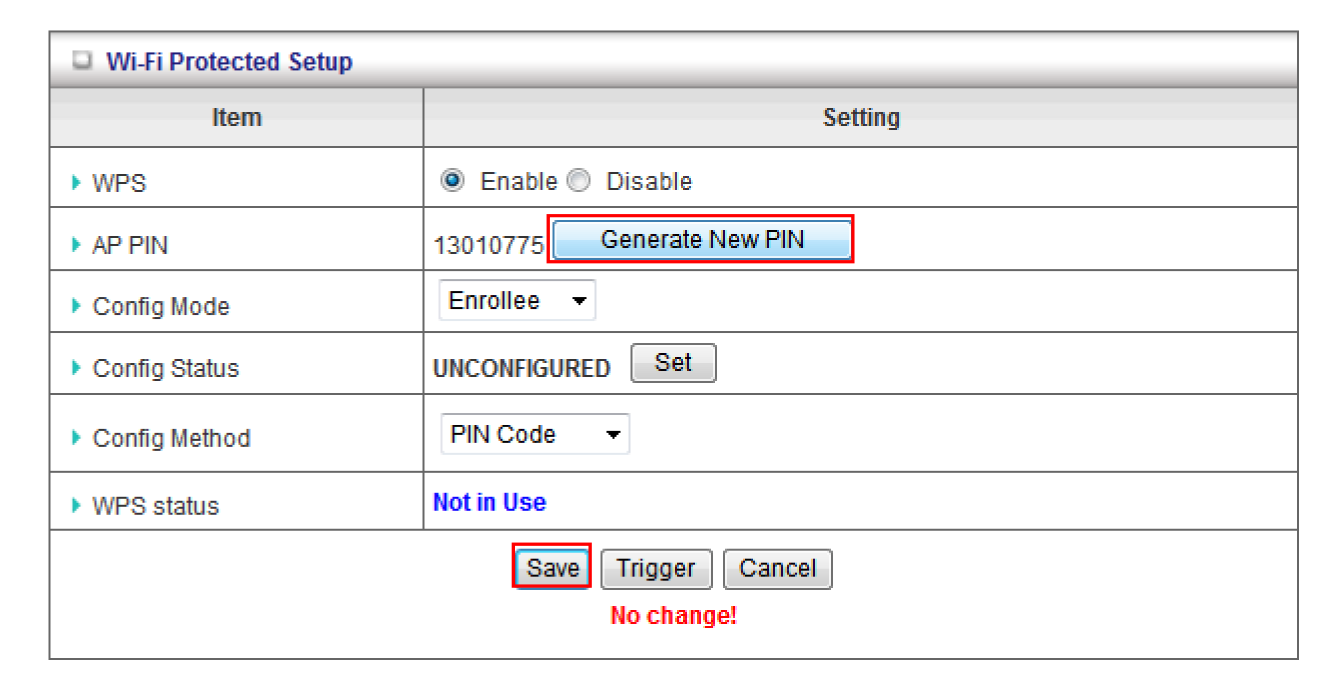
Sie verringert die Anzahl der Schritte, die ein Benutzer zur Konfiguration eines Netzwerks durchlaufen muss, und unterstützt zwei Methoden, mit denen die meisten Benutzer für die Konfiguration eines Netzwerks und Aktivierung von Sicherheitsfunktionen vertraut sind.

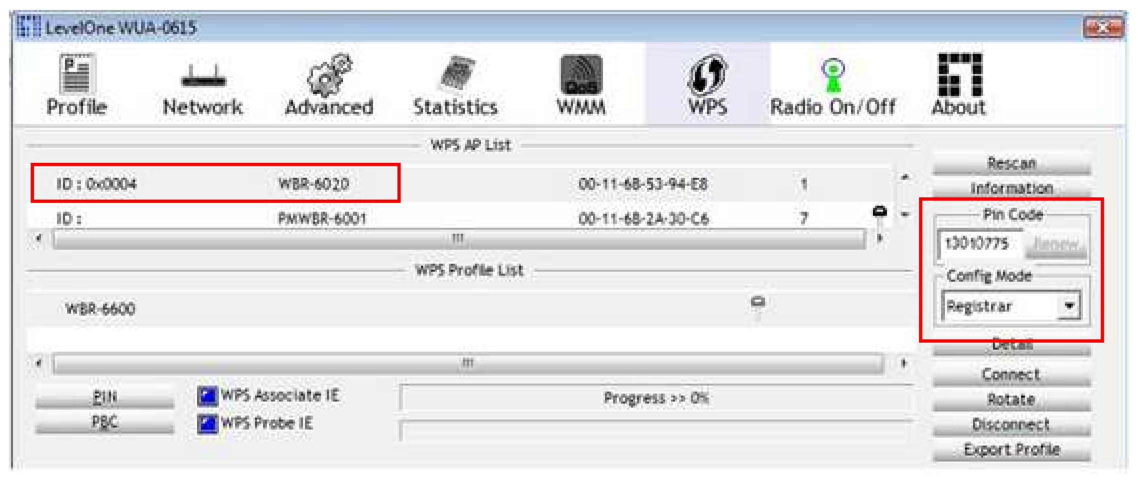
Vergewissern Sie sich, dass die Drahtlossicherheit auf dem WBR-6022 eingerichtet ist, bevor Sie die WPS-Funktionen initialisieren.

Einstellen der PIN-Nummer für den WBR-6022:
Vergewissern Sie sich, dass sich der Router im Modus “Enrollee” (Registrierender) befindet.

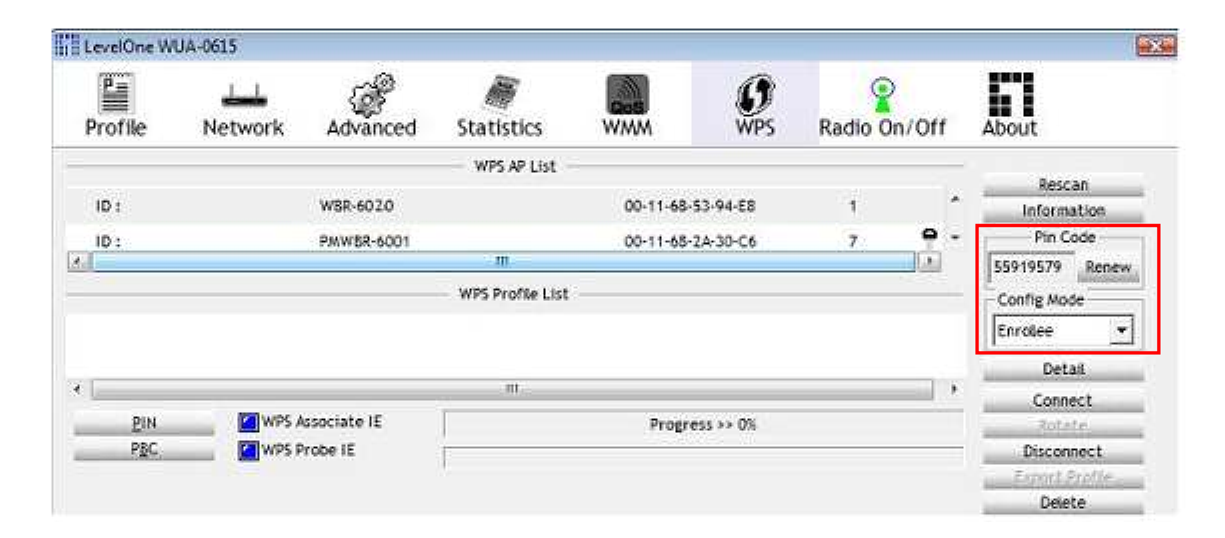
Klicken Sie auf die Schaltfläche “Generate New PIN” (Neue PIN erzeugen), um eine willkürliche neue PIN-Nummer für den WBR-6022 zu erstellen. Klicken Sie dann auf “Save” (Speichern), um die Einstellungen zu übernehmen.

Setzen Sie Ihren Drahtlosadapter als Registrar (Registrator) ein und geben Sie diese PIN-Nummer ein, um die WPS-Funktion zu initialisieren.

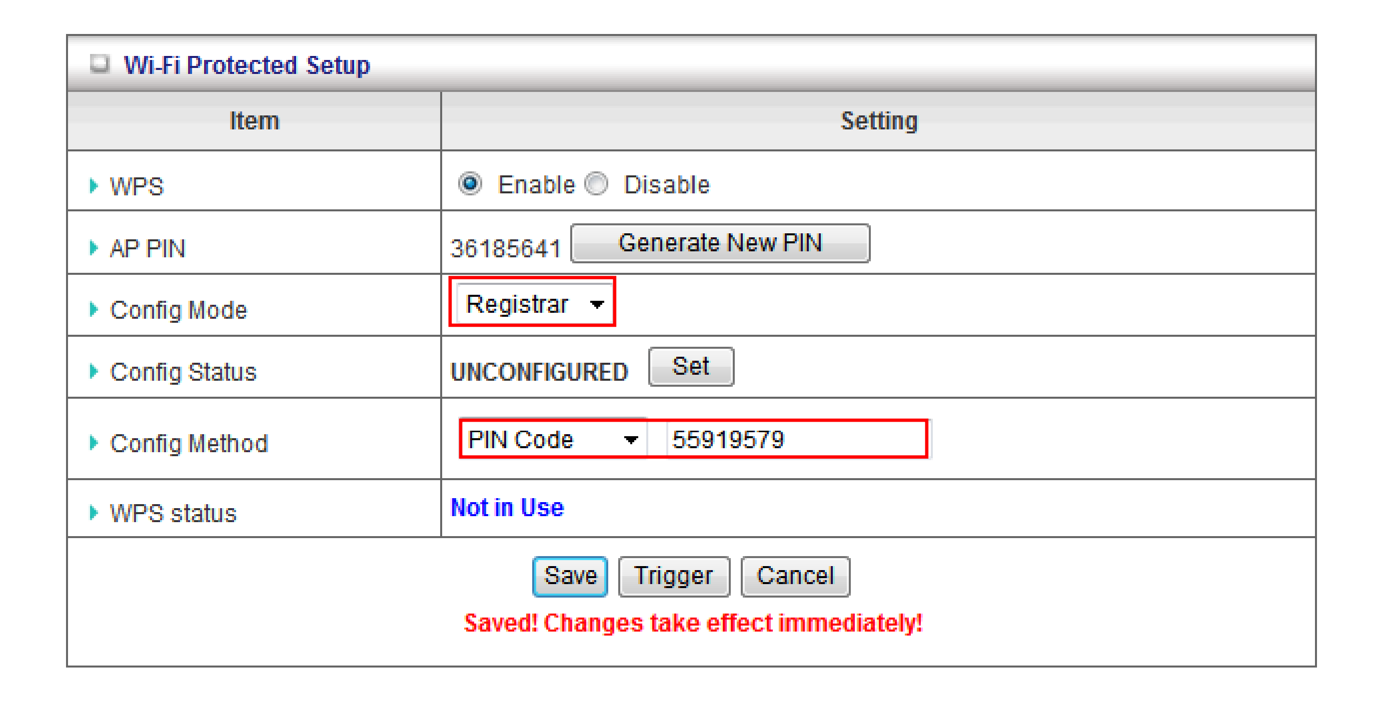




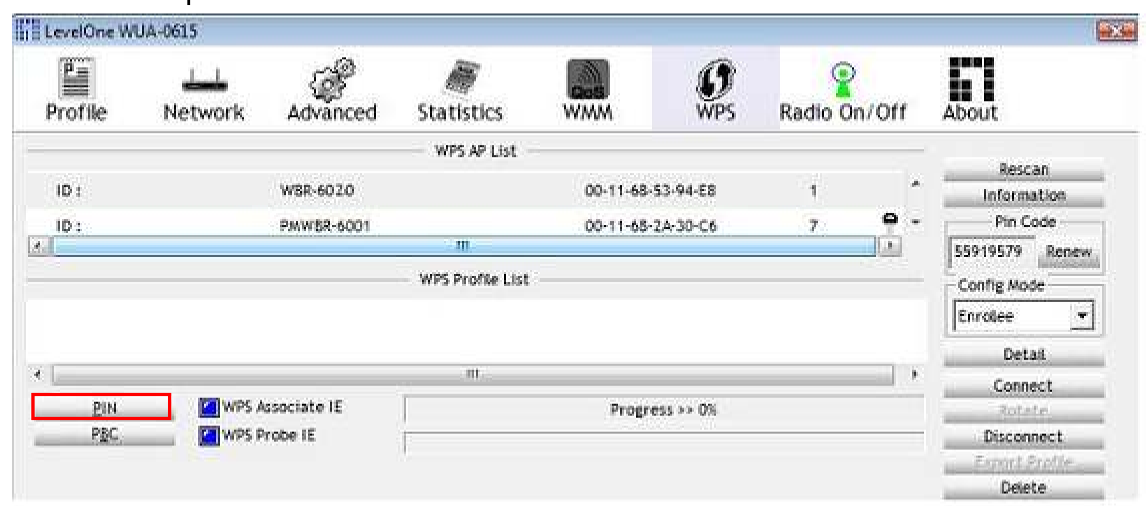
Eingabe der PIN-Nummer des Drahtlosadapters:
Es ist auch möglich, die PIN-Nummer zu verwenden, die Sie auf dem Drahtlosadapter eingestellt haben. Setzen Sie den Adapter als Enrollee (Registrierenden) ein und geben Sie die gewünschte PIN ein.



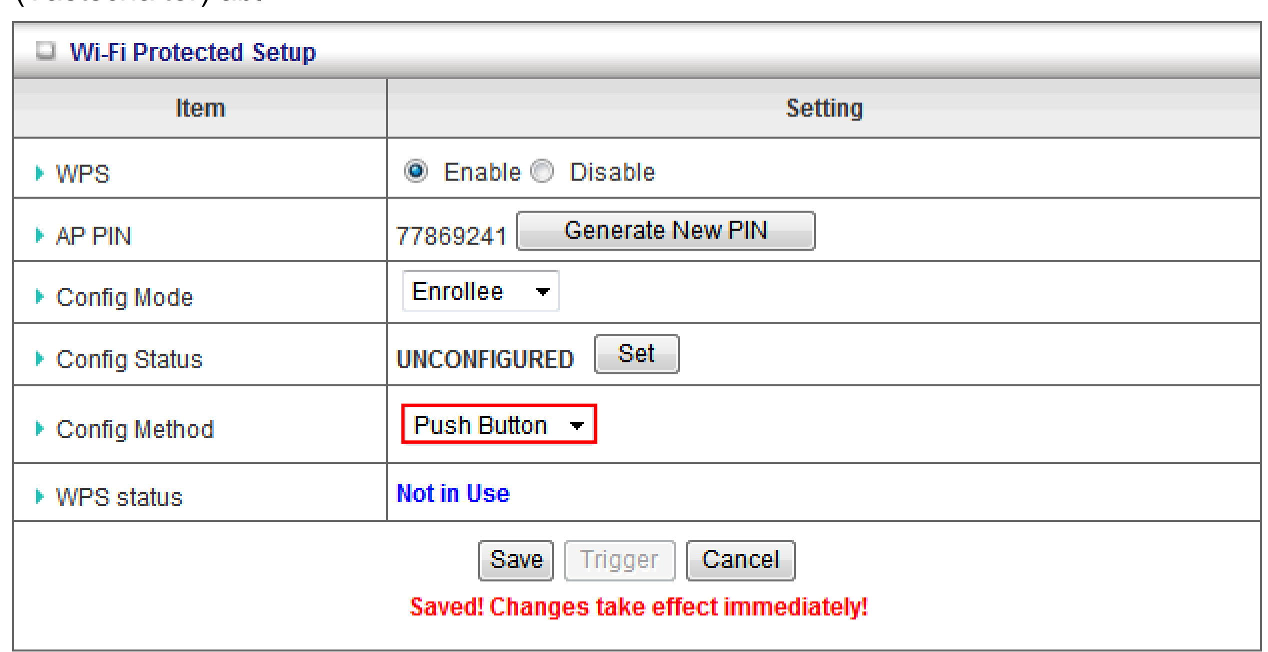
Geben Sie die PIN-Nummer des Registrierenden (Drahtlosadapter des Computers) ein und klicken Sie auf “Save” (Speichern).



Initialisieren Sie jetzt WPS, indem Sie die Schaltfläche “PIN” im Dienstprogramm des Drahtlosadapters anklicken.



Tastschaltermethode:
Ändern Sie den Punkt “Config Method” (Konfigurationsmethode) auf “Push Button” (Tastschalter) ab.



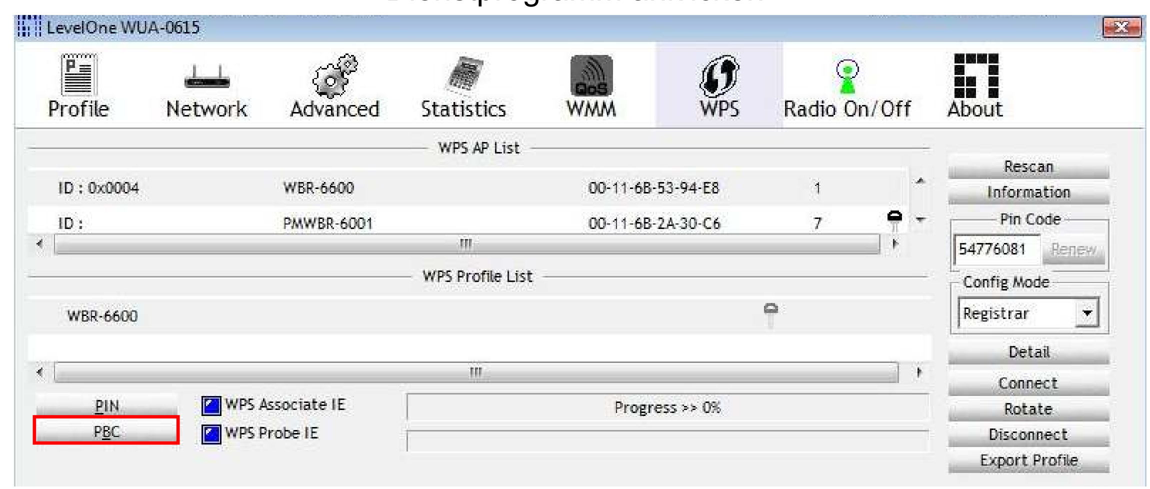
Drücken Sie dann die WPS-Taste vorne am Router, bis die WLAN-Anzeige anfängt zu blinken. WPS ist jetzt aktiviert.



Drücken und halten Sie dann 1 Sekunde lang die WPS-Taste Ihres Drahtlos-Clients.



Wenn Ihr Gerät keinen WPS-Tastschalter besitzt, können Sie die Software-Taste im Dienstprogramm anklicken.



WDS (Wireless Distribution System, Drahtloses Verteilungssystem von Verbindungen)

WDS-Betrieb wurde wie vom IEEE802.11-Standard definiert verfügbar gemacht. Mithilfe von WDS ist es möglich, sich mit Access Points (Zugangspunkten) drahtlos zu verbinden, wobei eine verdrahtete Infrastruktur auf Standorte ausgedehnt wird, wo keine Verkabelung möglich oder schlecht durchzuführen ist.

Für maximale Kompatibilität wird empfohlen, WDS nur auf denselben Modellen einzurichten, WBR-6022 in diesem Fall. Beachten Sie zudem, dass der Standard nur WEP-Verschlüsselung unterstützt.

Klicken Sie auf **Enable (Aktivieren)**, um die WDS-Funktion zu aktivieren.

Geben Sie dann die MAC-Adressen der anderen Zugangspunkte (APs) in den Feldern **Remote AP MAC (MAC vom ferngesteuerten AP)** ein. Oder Sie können die Adressen von der Liste **Scanned AP's MAC (MAC vom gescannten AP)** kopieren.

Klicken Sie auf **Save (Speichern)**, um die Einstellungen zu speichern, oder auf **Undo (Rückgängig)**, um sie zu ignorieren.

Hinweis: WDS unterstützt den drahtlosen WEP-Verschlüsselungsmodus.

WDS Setting [Help]

Item	Setting
Wireless Bridging	Enable Disable
Remote AP MAC 1	
Remote AP MAC 2	
Remote AP MAC 3	
Remote AP MAC 4	
Encryption type	None

Scaned AP's MAC -- select one -- Copy to Remote AP MAC --

Wireless AP List

ID	SSID	Channel	MAC Address
1	MeetingRoom	7	00:11:6B:B0:87:9C
2	WAP-0003	6	00:11:6B:60:6A:C5
3	ZyXEL	6	00:13:49:3D:DA:2D
4	QC-6000	11	00:11:6B:17:48:F6
5	WBR-6001TSD	11	00:11:6B:29:30:84
6	8FB1	6	00:09:7C:F1:F3:1B
7	MyPlace	2	00:18:84:A4:DB:06
8	TSD10	11	00:11:6B:39:A9:73
9	WAP-6010	11	00:05:9E:8D:85:C8
10	MyPlace	2	00:18:84:A4:DB:06

Save Undo Scan AP Back

Change Password (Kennwort ändern)

Auf dieser Seite können Sie das Kennwort für die Webkonfiguration des WBR-6022 ändern. Geben Sie das alte Kennwort ein (das werkseitig eingestellte Kennwort lautet **password**) und dann das neue Kennwort.

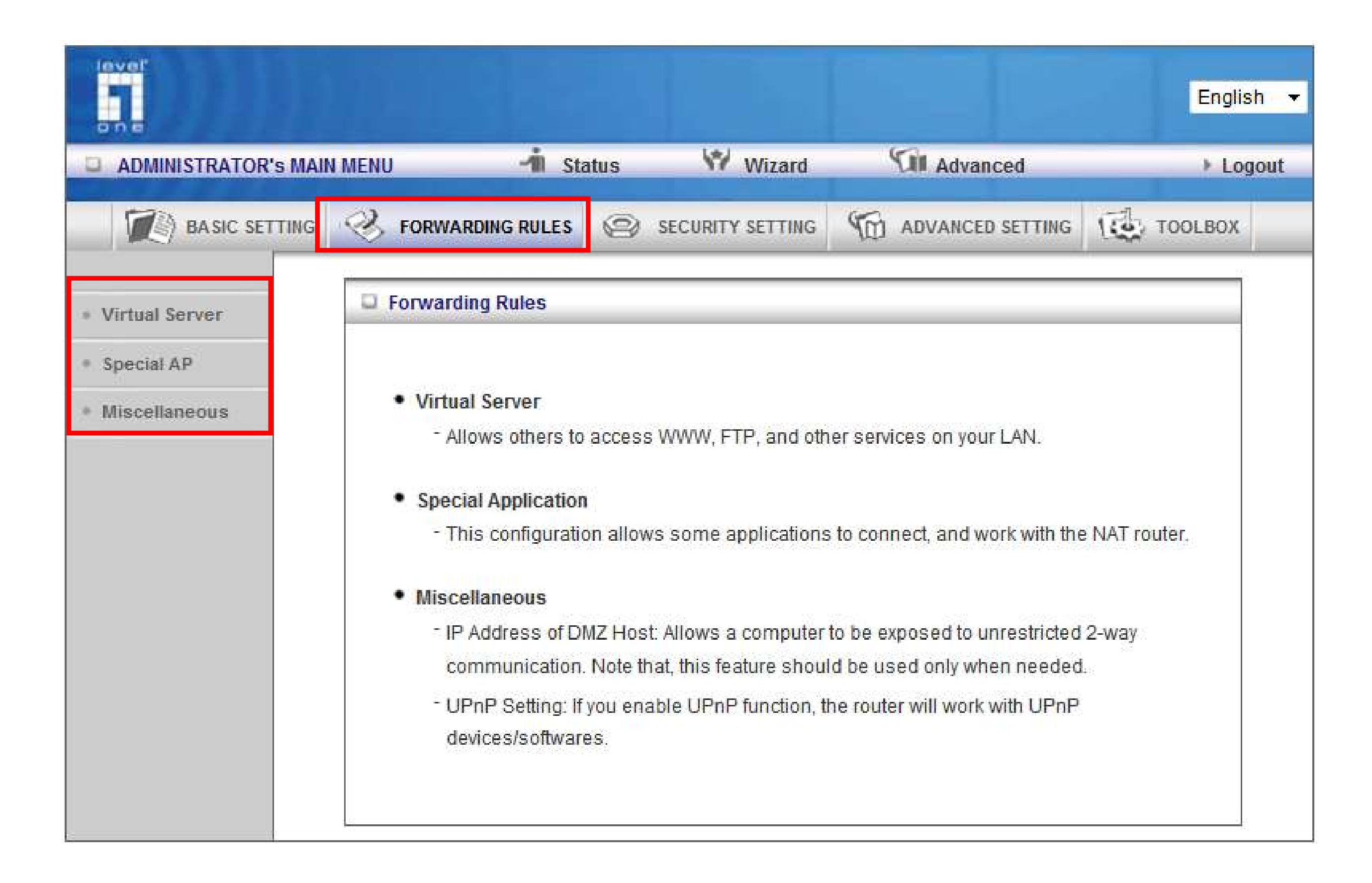


Nachdem Sie das Kennwort geändert haben, müssen Sie sich mit dem neuen Kennwort bei der Webkonfiguration anmelden.

Klicken Sie auf **Save (Speichern)**, um die Einstellungen zu speichern, oder auf **Undo (Rückgängig)**, um sie zu ignorieren.

Forwarding Rules (Weiterleitungsregeln)

Auf dieser Seite können Sie die Port-Weiterleitungsverwaltung des WBR-6022 konfigurieren. In dem Menü links bekommen Sie Zugriff auf die Seiten mit Einstellungen.

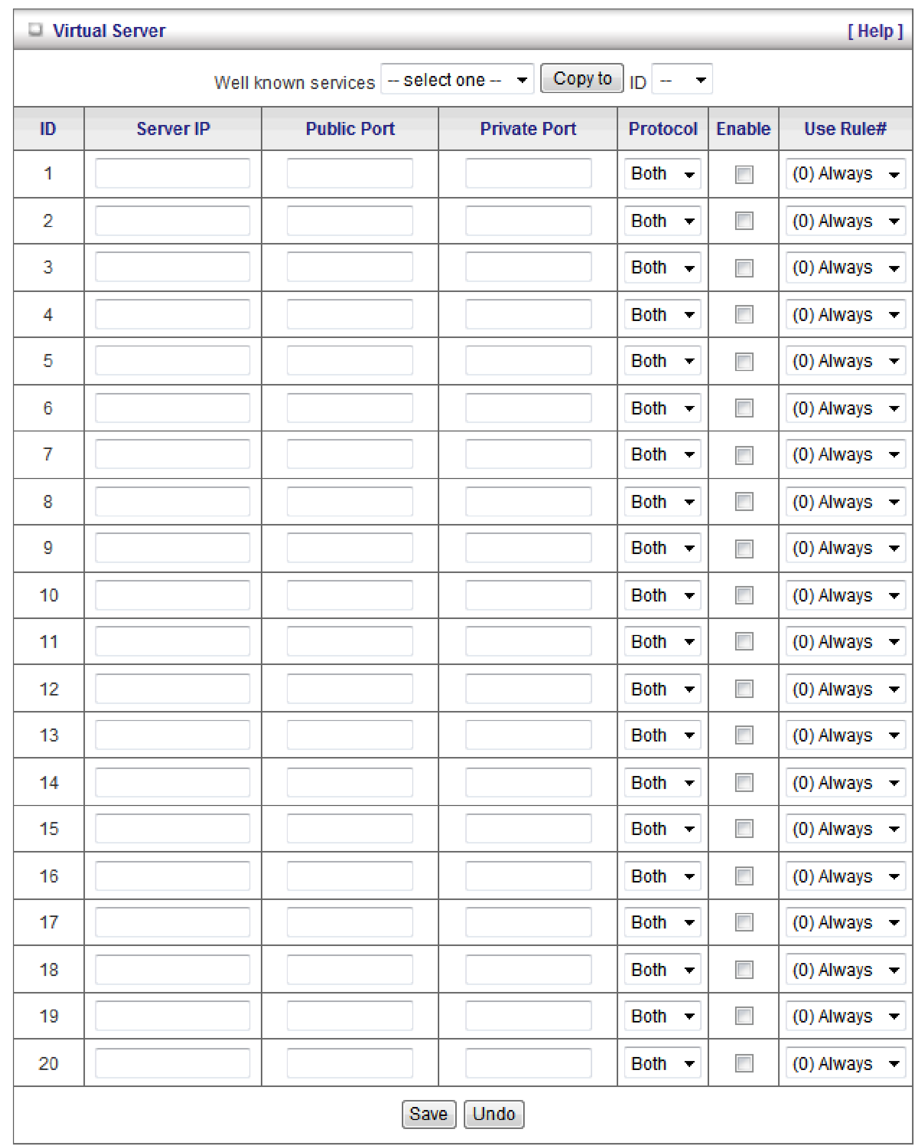


Die Funktion Port-Weiterleitung ist erforderlich, denn das NAT (Network Address Translation, Ersetzen von Netzwerkadressen) des Drahtlos-Routers wird den eingehenden Datenverkehr vom Internet zum LAN blockieren, wenn die spezielle Port-Zuordnung nicht in der NAT-Tabelle eingerichtet ist.

Dadurch werden Computer in Ihrem LAN mit einer Schutzstufe versehen, was jedoch Konnektivitätsprobleme verursacht, wenn Sie LAN-Ressourcen im Internet verfügbar machen möchten. Diese sind FTP-Server, Netzwerkserver für Spielprogramme oder andere Serveranwendungen.

Es gibt drei Methoden, das NAT zu umgehen, und LAN-Ressourcen im Internet zu aktivieren. Port-Weiterleitung (“Virtual Server”, Virtueller Server), Port-Auslösung(Seite “Special Applications”, Besondere Anwendungen) und DMZ-Host (Seite “Miscellaneous Items”, Verschiedenes).

Virtual Server (Virtueller Server)



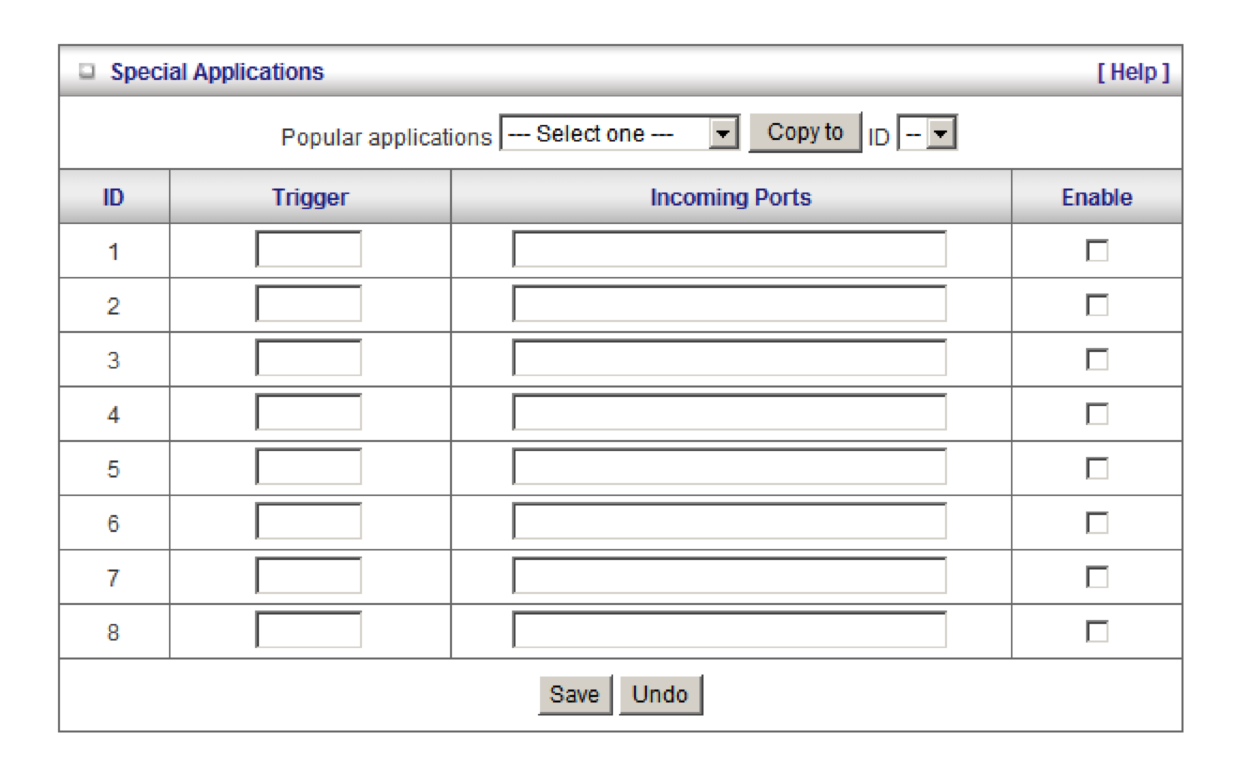
Ein virtueller Server ist als ein Dienst-Port definiert, wobei alle Anfragen an diesen Port zu dem Computer umgeleitet werden, der vom Server-IP vorgegeben ist. Ein virtueller Server arbeitet mit Zeitplanregeln und gibt Benutzern mehr Flexibilität bei der Zugangssteuerung. Beachten Sie hierzu die Details unter "Schedule Rule (Regelzeit programmieren)" (Advanced Setting (Erweiterte Einstellung) > Schedule (Zeitplan)).

Haben Sie z.B. einen FTP-Server (Port 21) unter 192.168.0.1, einen Webserver (Port 80) unter 192.168.0.2 und einen VPN-Server unter 192.168.0.6, müssen Sie die folgende Zuordnungstabelle für den virtuellen Server ausfüllen:

Sie können unterschiedliche Ports für die Verwendung von Public (Öffentlich) und Private (Privat) Quellen und Zielen festlegen.

Public Port (Öffentlicher Port)	Private Port (Privater Port)	Server IP (Server-IP)	Enable (Aktivieren)
20	21	192.168.0.2	V
80	80	192.168.0.3	V
1721	1723	192.168.0.6	V

Special Applications (Besondere Anwendungen)



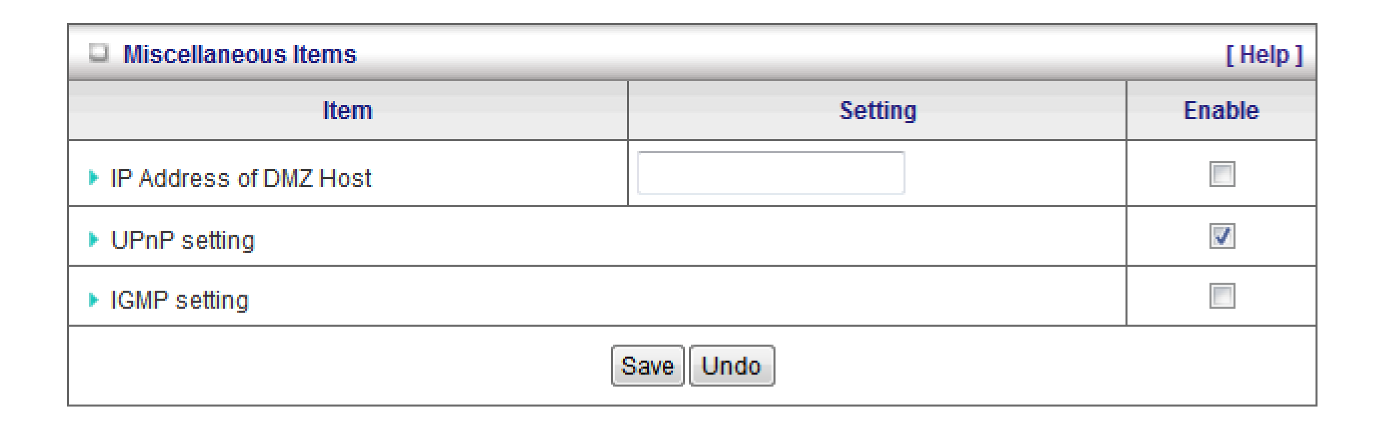
Einige Anwendungen benötigen mehrere Verbindungen, z.B. Internet-Spiele, Videokonferenzen, Internet-Telefonie, etc. Aufgrund der Firewall-Funktion können diese Anwendungen nicht mit WBR-6022 kooperieren. Mithilfe der Funktion **Special Applications (Besondere Anwendungen)** ist es einigen dieser Anwendungen möglich, auf diesem Gerät zu laufen. Sollte eine Anwendung dennoch weiterhin nicht funktionieren, können Sie versuchen, den Computer als **DMZ-Host** einzurichten. Siehe “Forwarding Rules” (Weiterleitungsregeln) > Abschnitt “Miscellaneous Items” (Verschiedenes).

1. **Trigger (Auslöser):** Die ausgehende Port-Nummer, die von der Anwendung ausgelöst wird.
2. **Incoming Ports (Eingehende Ports):** Wird das Auslösepaket erkannt, werden eingehende Pakete zu den festgelegten Port-Nummern gesandt und dürfen die Firewall passieren.

Sie erhalten den WBR-6022 bereits mit einigen vordefinierten Einstellungen für einige gängige Anwendungen. Um die vordefinierten Einstellungen zu verwenden, wählen Sie Ihre Anwendung aus der Liste aus, wählen Sie eine ungenutzte ID und klicken Sie auf **Copy (Kopieren)**, um die vordefinierte Einstellung Ihrer Liste hinzuzufügen.

Hinweis: Stets darf nur ein PC einen einzelnen Tunnel für Special Application (Sonderanwendung) verwenden.

Miscellaneous Items (Verschiedenes)



IP Address of DMZ Host (IP-Adresse vom DMZ-Host)

Hier können Sie den DMZ-Host (Demilitarized Zone, Entmilitarisierte Zone) einrichten. Es handelt sich hier um einen Computer, für den nicht die im WBR-6022 integrierte Firewall übernommen wurde. Hiermit wird der Computer auch für eine unbeschränkte Kommunikation dem Internet angezeigt.

Diese Einstellung wird am häufigsten für Internet-Spiele, Videokonferenzen, Internet-Telefonie und anderen Sonderanwendungen verwendet.

Um DMZ zu aktivieren, geben Sie die IP-Adresse des PCs ein und klicken Sie auf “Enable” (Aktivieren).

UPnP Setting (UPnP-Einstellung)

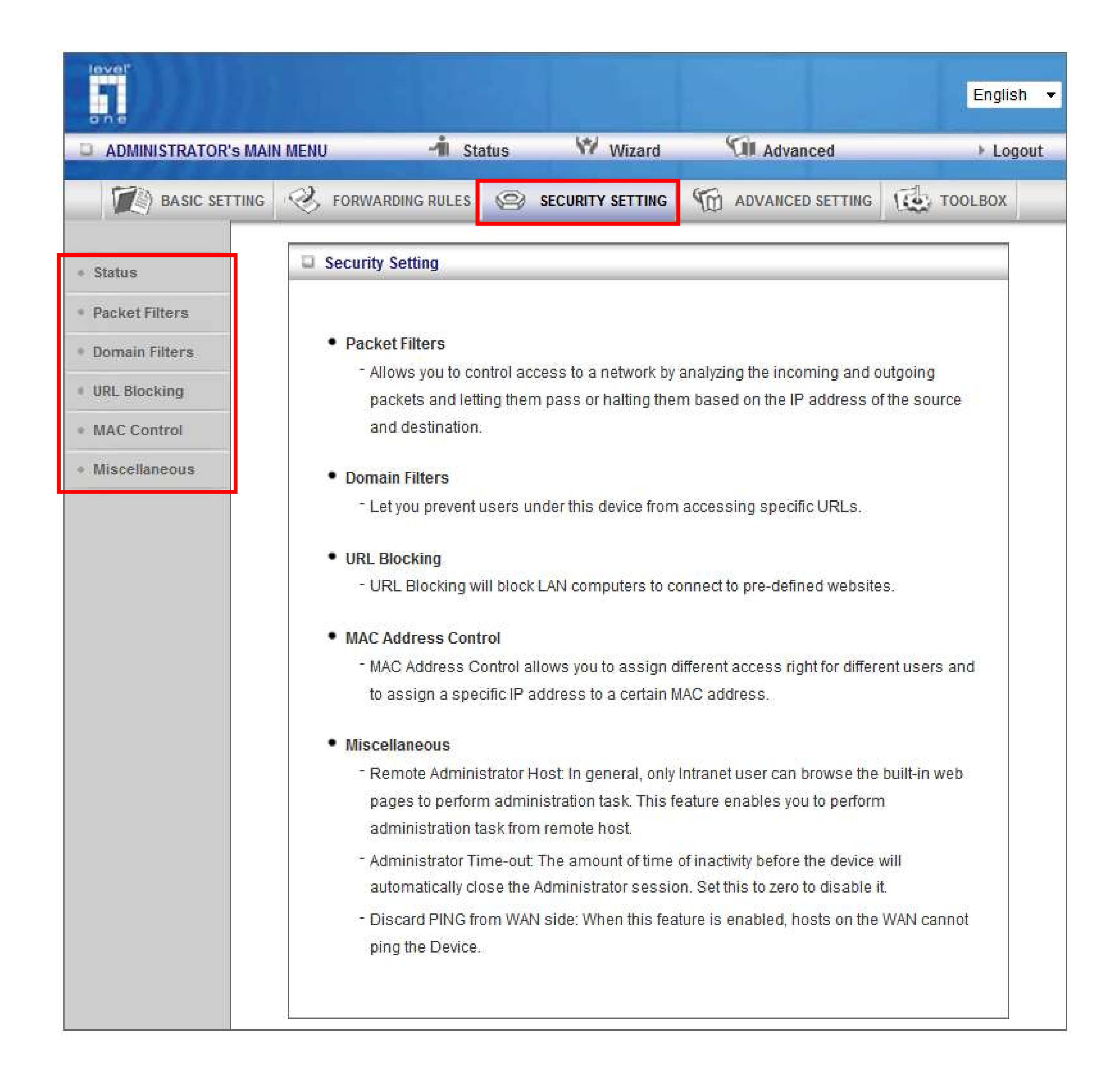
Der WBR-6022 unterstützt die universelle Plug-and-Play-Funktion (UPnP). Dies hängt jedoch von Ihrem Betriebssystem ab.

IGMP Setting (IGMP-Einstellung)

IGMP (Internet Group Management Protocol, Internet-Gruppenverwaltungsprotokoll) ist ein Protokoll, das für Multicasting-Anwendungen verwendet wird, wobei die Inhaltsdaten von einer Quelle zu einer Anzahl von Empfängern gesendet wird. Diese Funktion muss aktiviert werden, wenn sich Anwendungen in Ihrem LAN in einer Multicasting-Gruppe befinden.

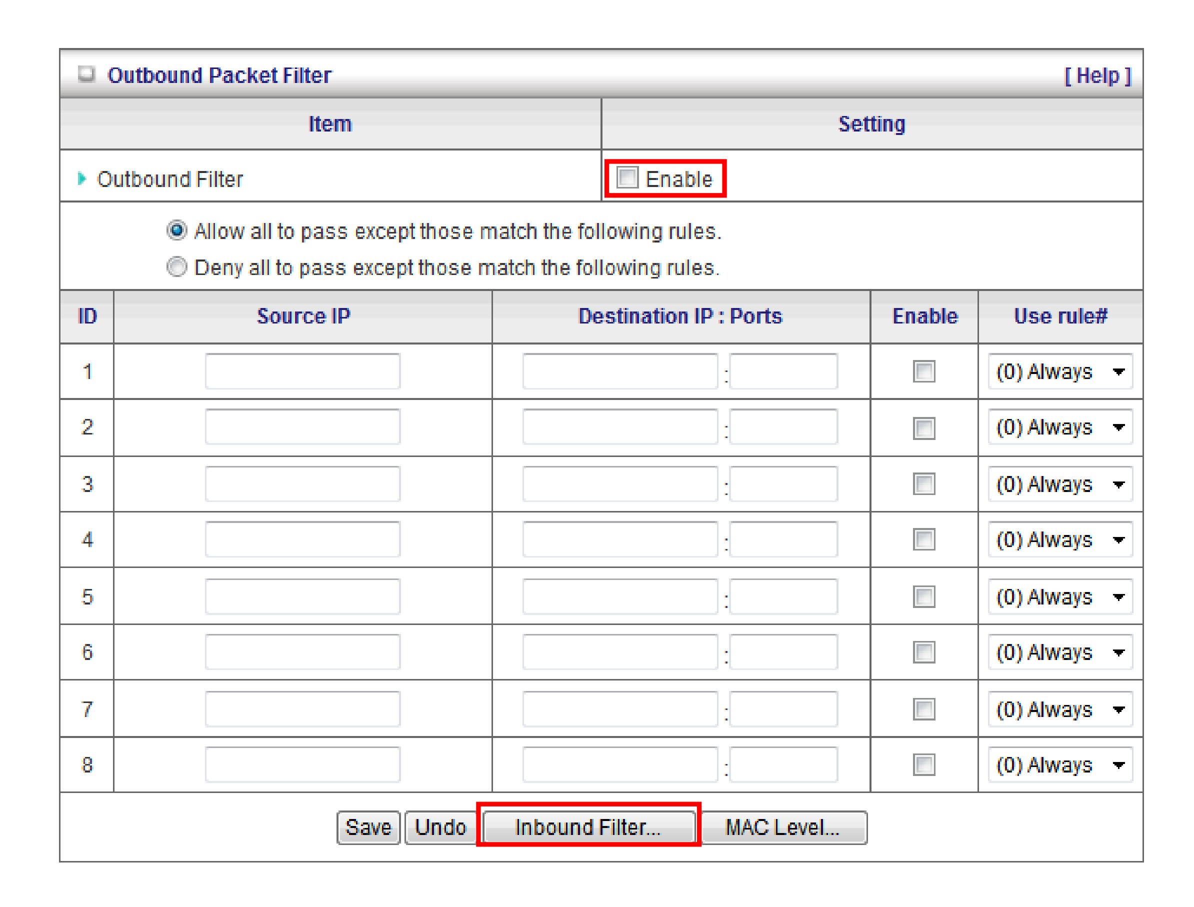
Security Setting (Sicherheitseinstellung)

Auf dieser Seite können Sie die Sicherheitsverwaltung des Geräts konfigurieren. Klicken Sie in das Menü links, um die Seite mit den dazugehörigen Einstellungen anzuzeigen.



Packet Filters (Paketfilter)

Mit “Packet Filters” (Paketfilter) können Sie kontrollieren, welche Pakete den WBR-6022 passieren dürfen. “Outbound Filter” (Ausgehender Filter) bezieht sich auf alle ausgehenden Pakete, während “Inbound Filter” (Eingehender Filter) sich nur auf die Pakete bezieht, die nur für virtuelle Server oder den DMZ-Host bestimmt sind.



Um “Outbound Filter” (Ausgehender Filter) zu aktivieren, versehen Sie das Kästchen **Enable (Aktivieren)** mit einem Häkchen.

Es gibt zwei Arten von Filterrichtlinien:

1. Alles darf passieren, außer das, was mit den vorgegebenen Regeln übereinstimmt.
2. Nichts darf passieren, außer das, was mit den vorgegebenen Regeln übereinstimmt.

Sie können 8 Regeln für jede Richtung vorgeben: eingehend oder ausgehend.

Für jede Regel können Sie Folgendes festlegen:

- Source IP (Quell-IP-Adresse)
- Quell-Port
- Destination IP (Ziel-IP-Adresse)
- Ziel-Port
- Protokoll: TCP oder UDP oder beides.
- Use Rule# (Regelnr. verwenden)

Für die Quell- oder Ziel-IP-Adresse können Sie eine einzelne IP-Adresse (192.168.0.1) oder einen IP-Adressbereich (192.168.0.100 – 192.168.0.200) festlegen. Ein Leerfeld steht für alle IP-Adressen.

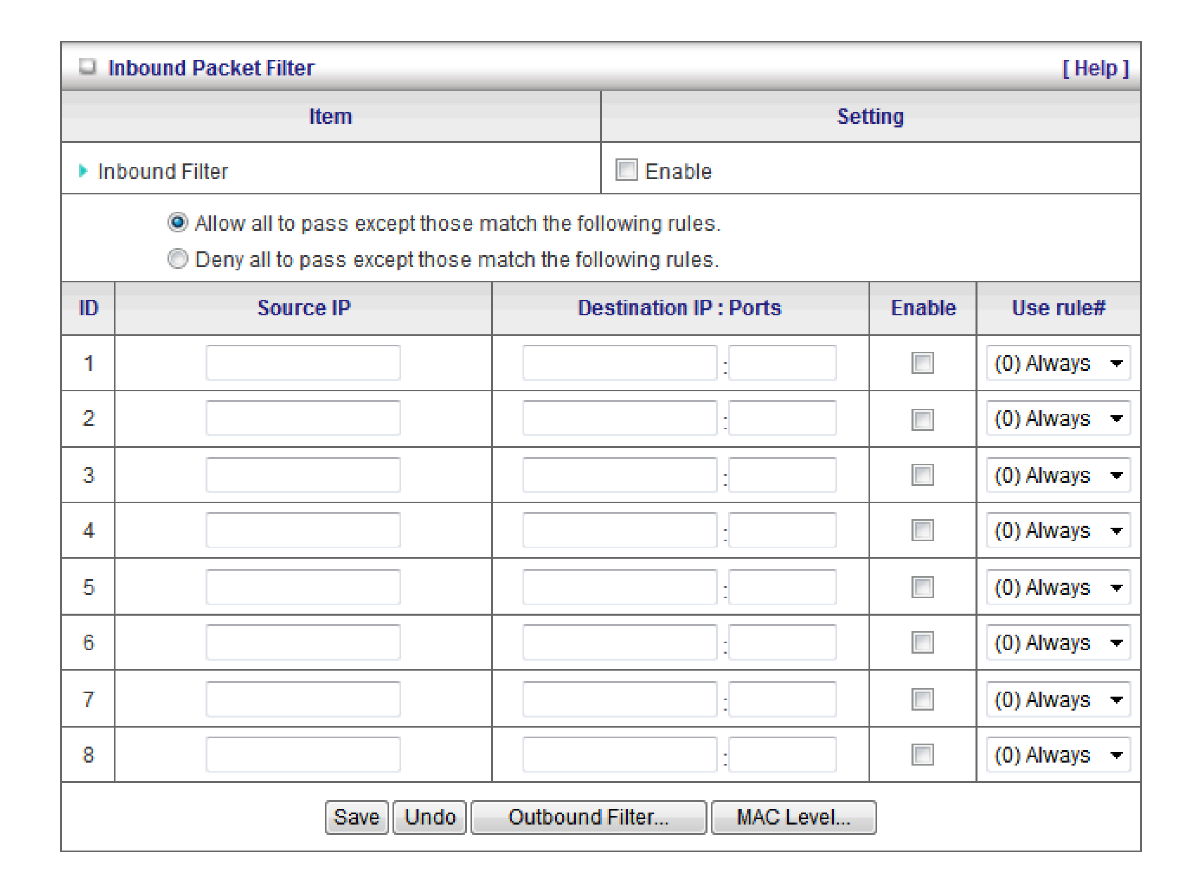
Für den Quell- oder Ziel-Port können Sie einen einzelnen Port (80) oder einen Port-Bereich (1000-1999) festlegen. Sie müssen auch ein "T" oder "U" voranstellen, um ein TCP- oder UDP-Protokoll zu kennzeichnen, z.B. T80, U53, U2000-2999. Wird kein Buchstabe vorangestellt, sind TCP und UDP definiert. Ein Leerfeld steht für alle Port-Adressen.

Packet Filter (Paketfilter) arbeitet auch mit Zeitplanregeln und gibt Benutzern mehr Flexibilität bei der Zugangssteuerung. Beachten Sie hierzu die Details unter “Schedule Rule (Regelzeit programmieren)” (Advanced Setting (Erweiterte Einstellung) > Schedule (Zeitplan)).

Jede Regel kann einzeln aktiviert oder deaktiviert werden.

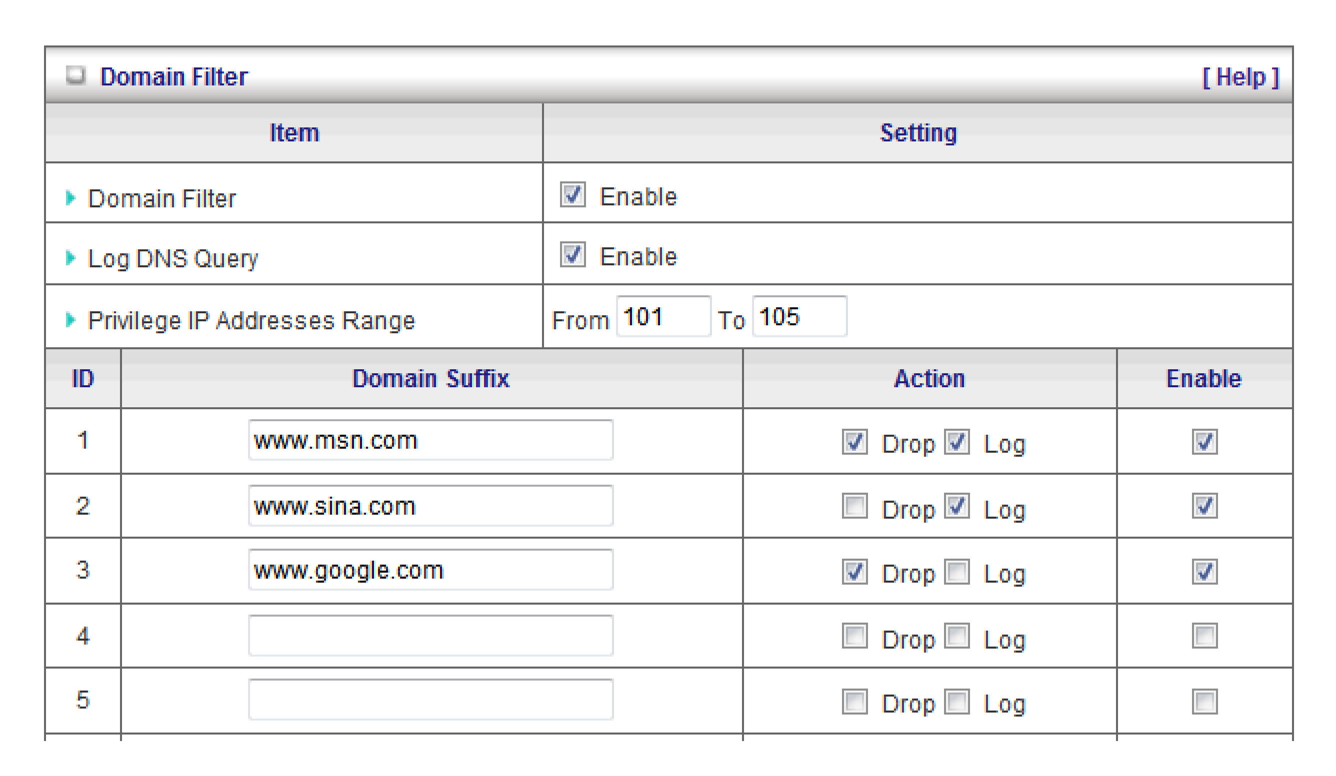
Inbound Filter (Eingehender Filter):

Um auf die Seite “Inbound Packet Filter” (Eingehender Paketfilter) zuzugreifen, klicken Sie unten auf der Seite auf **Inbound Filter (Eingehender Filter)**. Alle Einstellungen auf dieser Seite ähneln denen der ausgehenden Filter.



Domain Filter (Domänenfilter)

Mit Domain Filter (Domänenfilter) können Sie Benutzer daran hindern, auf bestimmte Domänenadressen (Websites) zuzugreifen.



Um "Domain Filter" (Domänenfilter) zu aktivieren, versehen Sie das Kästchen **Enable (Aktivieren)** mit einem Häkchen.

- **Log DNS Query (DNS-Abfrage protokollieren)**: Versehen Sie das Kästchen mit einem Häkchen, wenn Sie den Zugriff von Benutzern auf bestimmte URLs protokollieren möchten.
- **Privilege HOST/Netmask (Privileg-HOST/Netzmaske):** Legt eine Gruppe von Computern fest, die privilegierten Zugang zum Internet ohne Beschränkungen haben.
- **Domain Suffix (Domänennachsilbe)**: Eine Nachsilbe von URLs, die beschränkt werden sollen, wie z.B. ".com", "xxx.com".
- **Action (Handlung)**: Kennzeichnet die Handlung, die der WBR-6022 ergreifen soll, wenn jemand auf eine URL zugreift, auf welche die Bedingung der Domänennachsilbe zutrifft. Versehen Sie das Kästchen **Drop (Ignorieren)** mit einem Häkchen, wenn Sie den Zugriff blockieren möchten, und/oder versehen Sie das Kästchen **Log (Protokollieren)** mit einem Häkchen, um den Zugriff zu protokollieren.

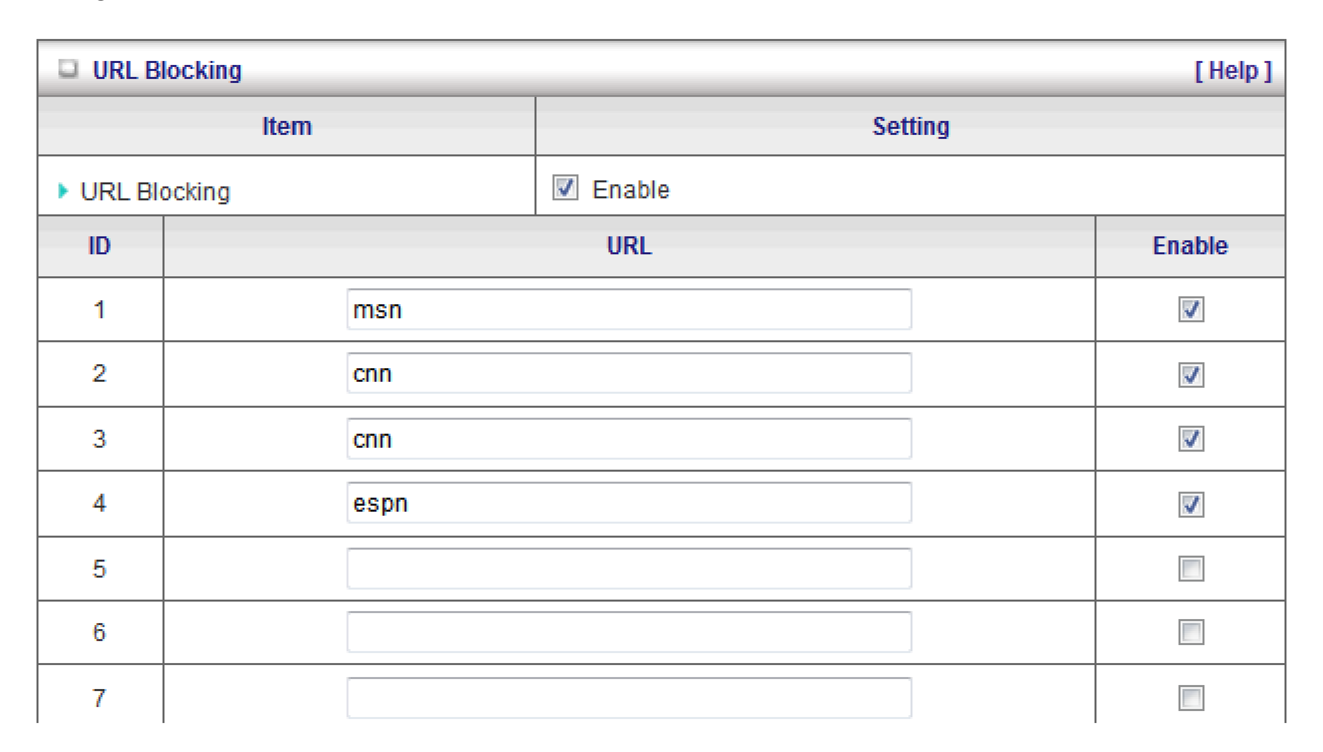
Im obigen Beispiel:

1. Wird die URL, die "www.msn.com" enthält, blockiert und die Handlung wird in einer Protokolldatei aufgezeichnet.
2. Wird die URL, die "www.sina.com" enthält, nicht blockiert, aber die Handlung wird in einer Protokolldatei aufgezeichnet.
3. Wird die URL, die "www.google.com" enthält, blockiert, aber die Handlung wird nicht in einer Protokolldatei aufgezeichnet.
4. Können die IP-Adressen X.X.X.1~ X.X.X.20 unbeschränkt auf das Netzwerk zugreifen.

URL Blocking (URL-Blockierung)

URL Blocking (URL-Blockierung) blockiert LAN-Computer, so dass sie sich nicht mit einer vordefinierten Website verbinden können. Der wesentliche Unterschied zwischen Domain Filter (Domänenfilter) und URL Blocking (URL-Blockierung) ist, dass für den Domänenfilter die Eingabe von Nachsilben erforderlich ist (z.B.: xxx.com, ttt.net), während für die URL-Blockierung nur ein Schlüsselwort eingegeben werden muss.

Anders ausgedrückt: der Domänenfilter kann bestimmte Websites blockieren, während die URL-Blockierung Hunderte von Websites nur mit einem Schlüsselwort blockiert.



URL Blocking [Help]

Item	Setting
URL Blocking	☑ Enable

ID	URL	Enable
1	msn	☑
2	cnn	☑
3	cnn	☑
4	espn	☑
5		☐
6		☐
7		☐

Um “URL Blocking” (URL-Blockierung) zu aktivieren, versehen Sie das Kästchen **Enable (Aktivieren)** mit einem Häkchen.

Um eine Regel für die URL-Blockierung einzurichten, benötigen Sie:

- **URL:** Wenn ein Teil der URL-Website mit dem vordefinierten Wort übereinstimmt, wird die Verbindung blockiert.
- **Enable (Aktivieren):** Versehen Sie dieses Kästchen mit einem Häkchen, um die Regel zu aktivieren.

Im obigen Beispiel:

1. Wird die URL, die “msn” enthält, blockiert und die Handlung wird in einer Protokolldatei aufgezeichnet.

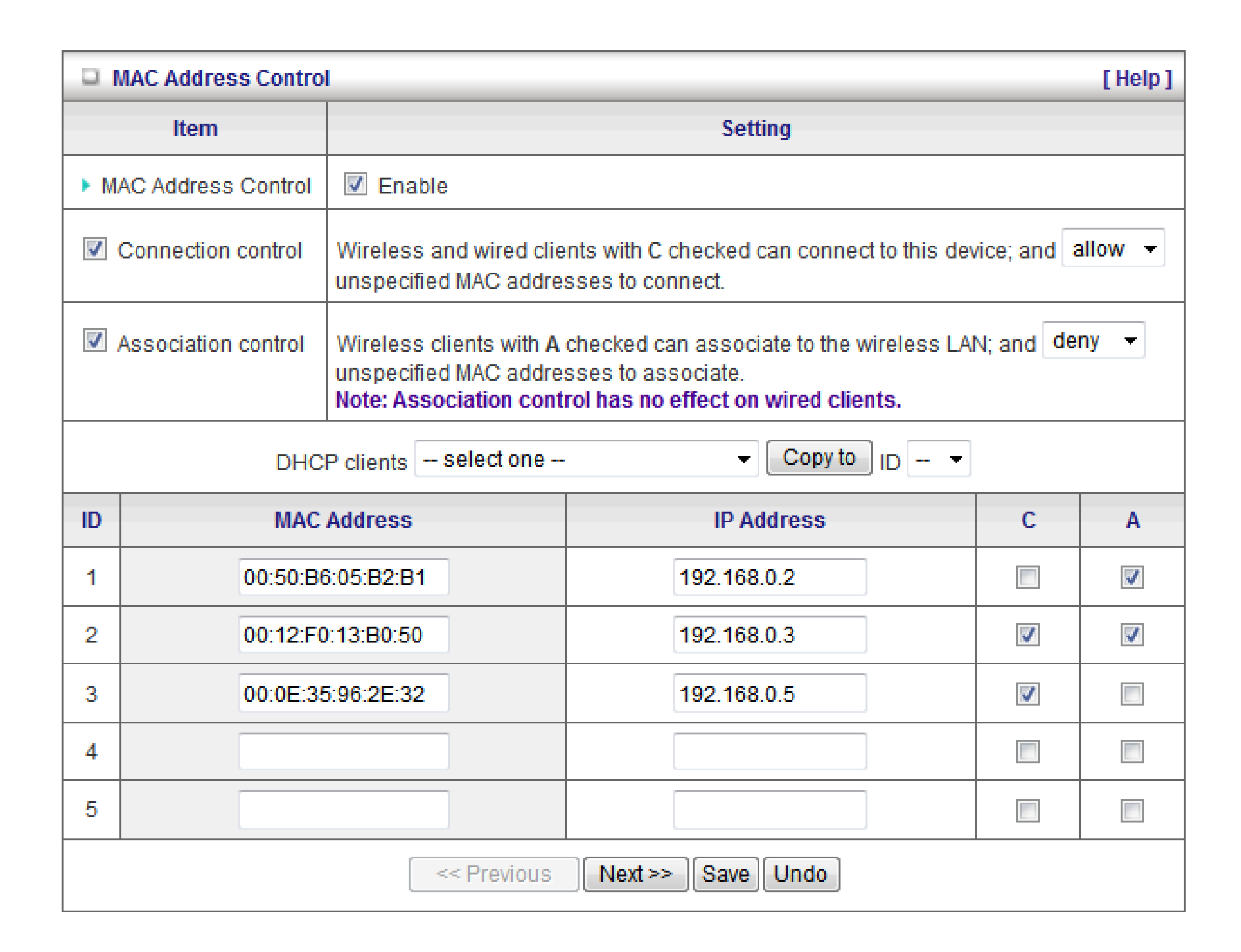
2. Wird die URL, die “sina” enthält, blockiert, aber die Handlung wird in einer Protokolldatei aufgezeichnet.

3. Wird die URL, die “cnnsi” enthält, nicht blockiert, aber die Handlung wird in einer Protokolldatei aufgezeichnet.

4. Wird die URL, die “espn” enthält, blockiert, aber die Handlung wird in einer Protokolldatei aufgezeichnet.

MAC Address Control (MAC-Adressenkontrolle)

Mit Domain Filter (Domänenfilter) können Sie Benutzer daran hindern, auf bestimmte Domänenadressen (Websites) zuzugreifen.



Um “MAC Address Control” (MAC-Adressenkontrolle) zu aktivieren, versehen Sie das Kästchen **Enable (Aktivieren)** mit einem Häkchen.

Es gibt zwei Arten von Kontrollen:

- **Connection Control (Verbindungskontrolle):** Hiermit wird kontrolliert, welche verdrahteten und drahtlosen Clients sich mit diesem Gerät verbinden dürfen. Wird einem Client der Zugang verweigert, bedeutet dies, dass der Client auch keinen Zugang zum Internet hat. Legen Sie mit “allow” (zulassen) oder “deny” (verweigern) die entsprechende Zugangsweise von Clients fest, deren MAC-Adressen nicht aufgelistet sind.
- **Association Control (Zuordnungskontrolle):** Hiermit wird kontrolliert, welcher drahtlose Client diesem WBR-6022 zugeordnet wird. Wird ein Client abgewiesen, bedeutet dies, dass der Client keine Daten über diesen WBR-6022 senden oder empfangan kann. Legen Sie mit “allow” (zulassen) oder “deny” (verweigern) die entsprechende Zuordnungsweise von Clients fest, deren MAC-Adressen sich nicht in der Liste zur Zuordnung zum Drahtlosnetzwerk befinden.

MAC Address (MAC-Adresse)	Die MAC-Adresse kennzeichnet einen bestimmten Client.
IP Address (IP-Adresse)	Die erwartete IP-Adresse vom entsprechenden Client. Lassen Sie dieses Feld leer, wenn Ihnen seine IP-Adresse nicht wichtig ist.
C	Haben Sie das Kästchen "**Connection control**" **(Verbindungskontrolle)** abgehakt, kann sich der entsprechende Client mit diesem Gerät verbinden, wenn "**C**" mit einem Häkchen versehen ist.
A	Haben Sie das Kästchen "**Association control**" **(Zuordnungskontrolle)** abgehakt, kann der entsprechende Client dem Drahtlos-Lan zugeordnet werden, wenn "**A**" mit einem Häkchen versehen ist.

Auf dieser Seite machen wir folgendes Kombinationsfeld und eine Schaltfläche als Eingabehilfe für die MAC-Adresse verfügbar.



Sie können im Kombinationsfeld “DHCP clients” (DHCP-Clients) einen bestimmten Client auswählen und dann die Schaltfläche “Copy to” (Kopieren nach) anklicken, um die MAC-Adresse vom ausgewählten Client zu der ID zu kopieren, die im Kombinationsfeld “ID” gewählt wurde.

Blättern von Seiten mit “Previous” (Zurück) und “Next” (Weiter)

Um die Einrichtungsseite einfach und übersichtlich zu gestalten, haben wir die “Kontrolltabelle” in mehrere Seiten unterteilt. Sie können mit diesen Schaltflächen zu den einzelnen Seiten blättern.

Beispiel:

In diesem Fall sind drei Clients in der Tabelle aufgelistet. Client 1 und 2 sind drahtlos und Client 3 ist verdrahtet.

1. Die Funktion “MAC Address Control” (MAC-Adressenkontrolle) ist aktiviert.
2. **Connection Control (Verbindungskontrolle)** ist aktiviert und allen verdrahteten und drahtlosen Clients, die nicht in der Kontrolltabelle aufgelistet sind, ist es "gestattet", sich mit diesem Gerät zu verbinden.
3. **Association Control (Zuordnungskontrolle)** ist aktiviert und allen drahtlosen Clients, die nicht in der Kontrolltabelle aufgelistet sind, wird eine Zuordnung zum Drahtlos-Lan "verweigert".
4. Client 1 und 3 haben feststehende IP-Adressen, die entweder vom DHCP-Server dieses Geräts stammen oder manuell zugewiesen wurden:

   ID 1 - "00-50-B6-05-B2-B1" --> 192.168.0.2
   ID 3 - "00-0E-35-96-2E-32" --> 192.168.0.5

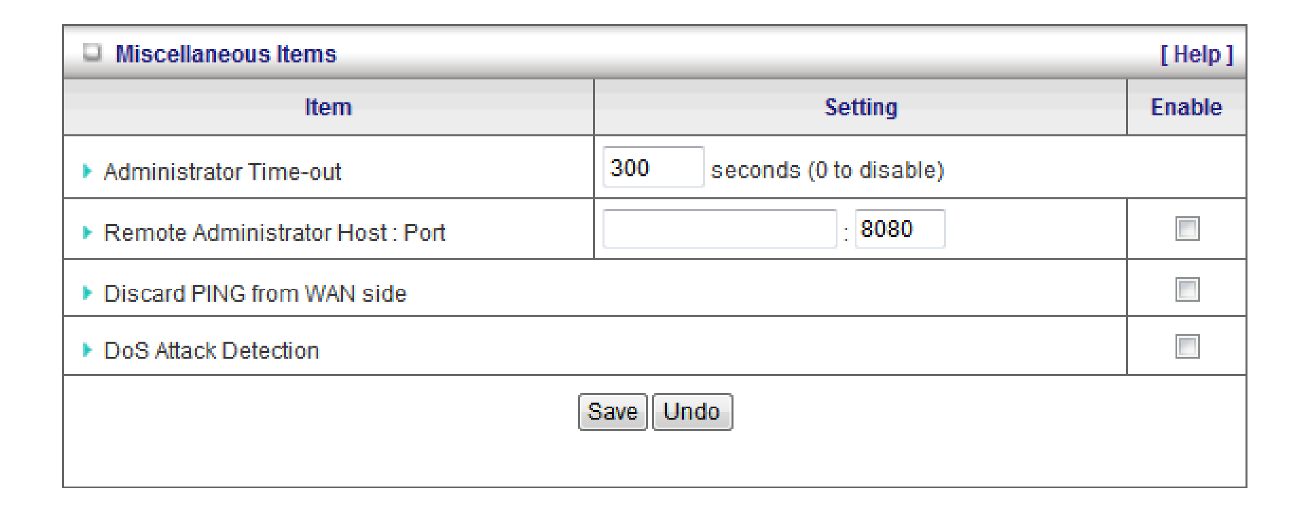
   Client 2 bezieht seine IP-Adresse vom IP-Adresspool, der auf der Seite "DHCP Server" (DHCP-Server) angegeben wurde, oder ihm kann eine statische IP-Adresse manuell zugewiesen worden sein.

Wenn Client 3 z.B. versucht, eine IP-Adresse zu verwenden, die von der in der Kontrolltabelle aufgelisteten Adresse abweicht (192.168.0.5), wird ihm die Verbindung mit dem WBR-6022 verweigert.

5. Client 2 und 3 sowie anderen verdrahteten Clients, deren MAC-Adressen nicht in der Kontrolltabelle aufgelistet sind, ist es gestattet, sich mit diesem Gerät zu verbinden. Aber Client 1 darf sich nicht mit diesem Gerät verbinden.
6. Client 1 und 2 ist es gestattet, dem Drahtlos-LAN zugeordnet zu werden, aber einem Drahtlos-Client, dessen MAC-Adresse nicht in der Kontrolltabelle aufgelistet ist, wird die Zuordnung zum Drahtlos-LAN verweigert. Client 3 ist ein verdrahteter Client und unterliegt daher nicht der Zuordnungskontrolle.

Miscellaneous Items (Verschiedenes)

Auf dieser Seite können Sie verschiedenartige Sicherheitseinstellungen ändern.



Administrator Time-out (Administrator-Auszeit): Kennzeichnet die Zeitlänge ohne Aktivität, nach derem Ablauf der Benutzer von den Seiten für Webkonfiguration abgemeldet wird. Setzen Sie diese Funktion auf Null, um sie zu deaktivieren.

Remote Administrator Host/Port (Ferngesteuerter Administrator-Host/Port): Per Standard ist es nur den LAN-Benutzern gestattet, die integrierten Seiten der Webkonfiguration für administrative Aufgaben aufzurufen. Mit dieser Funktion können Sie diese administrativen Aufgaben vom Internet aus ausführen. Ist diese Funktion aktiviert, darf nur die angegebene IP-Adresse eine ferngesteuerte Administration vornehmen. Ist das Feld für IP-Adressvorgabe leer, kann jeder beliebige Host sich mit diesem Gerät für administrative Aufgaben verbinden.

Aus Sicherheitsgründen geben Sie hier nur eine IP-Adresse an oder geben Sie mit der Schreibweise “/nn” für Subnetzmaskenbits eine Gruppe vertrauenswürdiger IP-Adressen ein. Zum Beispiel: "10.1.2.0/24".

HINWEIS: Bei Aktivierung der ferngesteuerten Administration wechselt der Webserver-Port zu 80. Sie können den Webserver-Port auf einen anderen Port abändern.

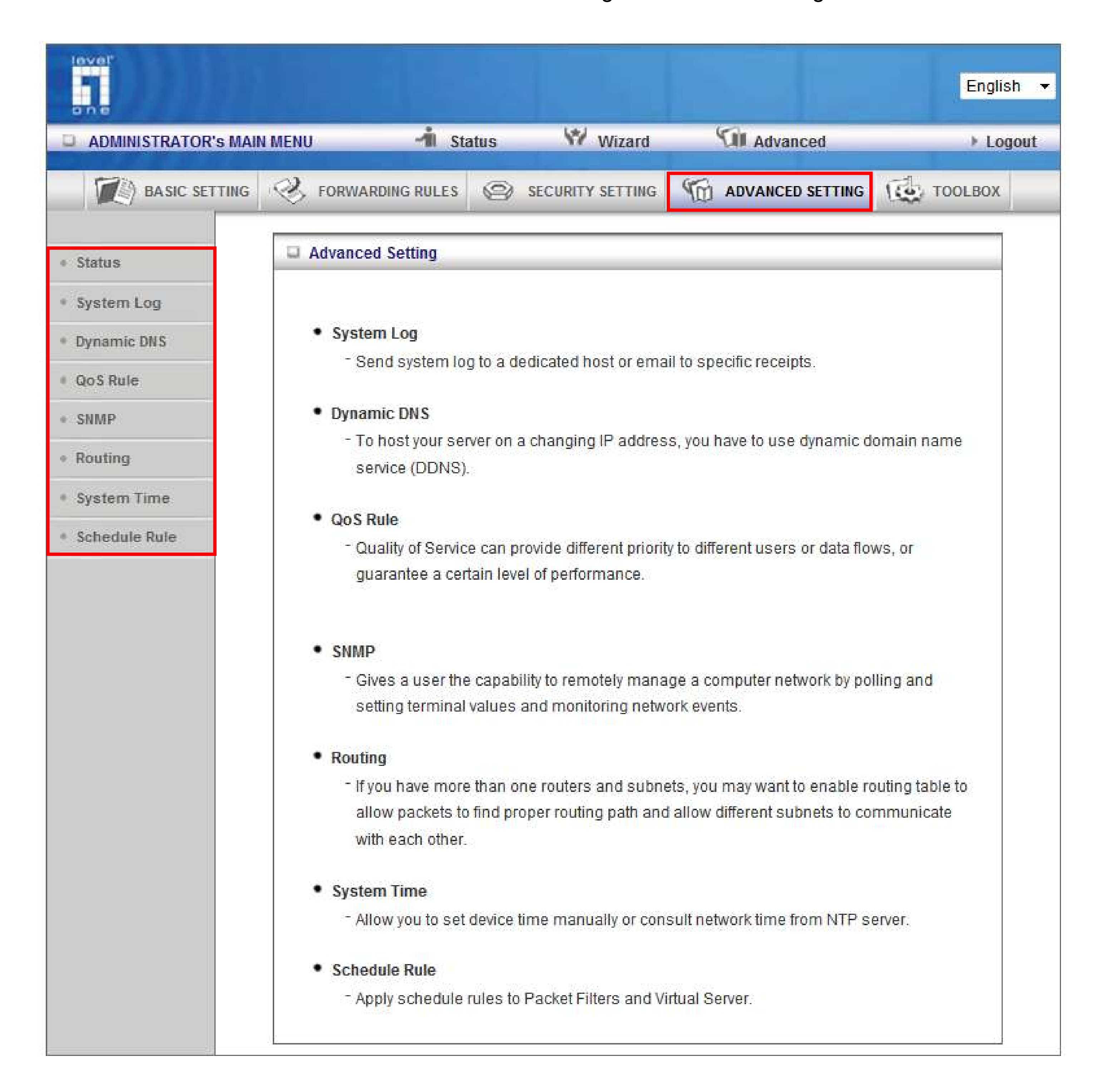
Discard PING from WAN side (PING von WAN-Seite ignorieren): Ist dieser Punkt aktiviert, kann kein Host im WAN diesen MobilSpot™ pingen.

DoS Attack Detection (DoS-Angriffsmeldung):

Wenn diese Funktion aktiviert ist, meldet und protokolliert der Router einen DoS-Angriff vom Internet. Derzeit kann der Router folgende DoS-Angriffe erkennen: SYN Attack, WinNuke, Port Scan, Ping of Death, Land Attack, etc.

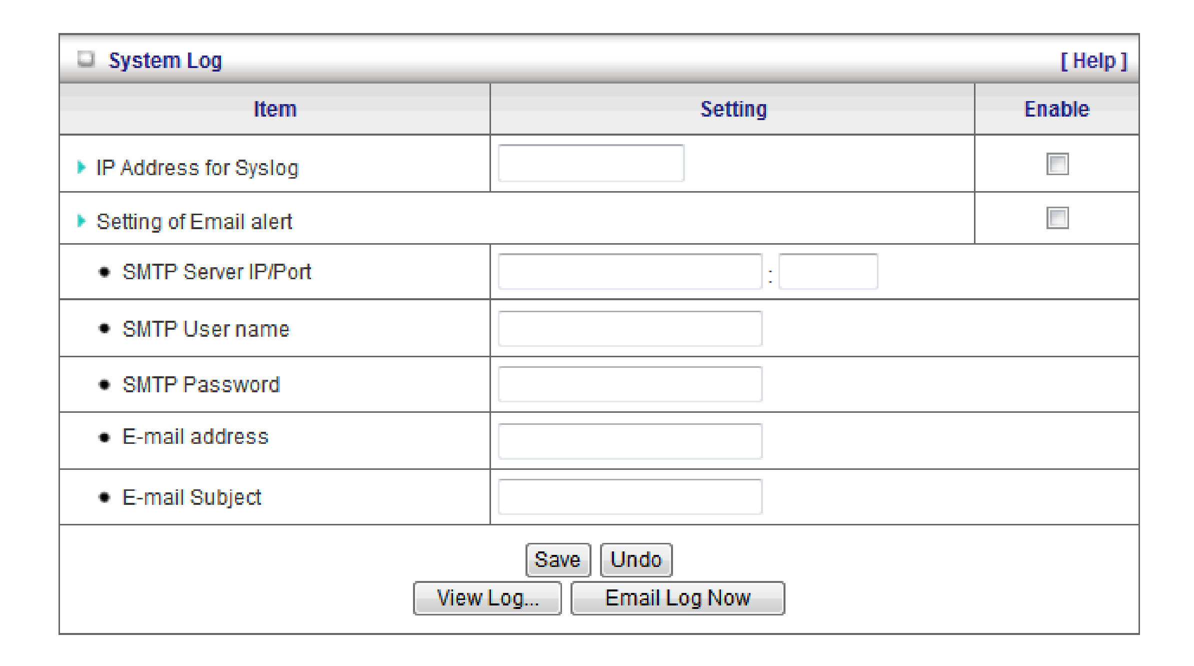
Advanced Settings (Erweiterte Einstellungen)

Auf diesen Seiten können Sie die erweiterten Einstellungen des Geräts konfigurieren.



System Log (Systemprotokoll)

Der WBR-6022 unterstützt Syslog (mittels UDP-Paketen) und E-Mailwarnung.



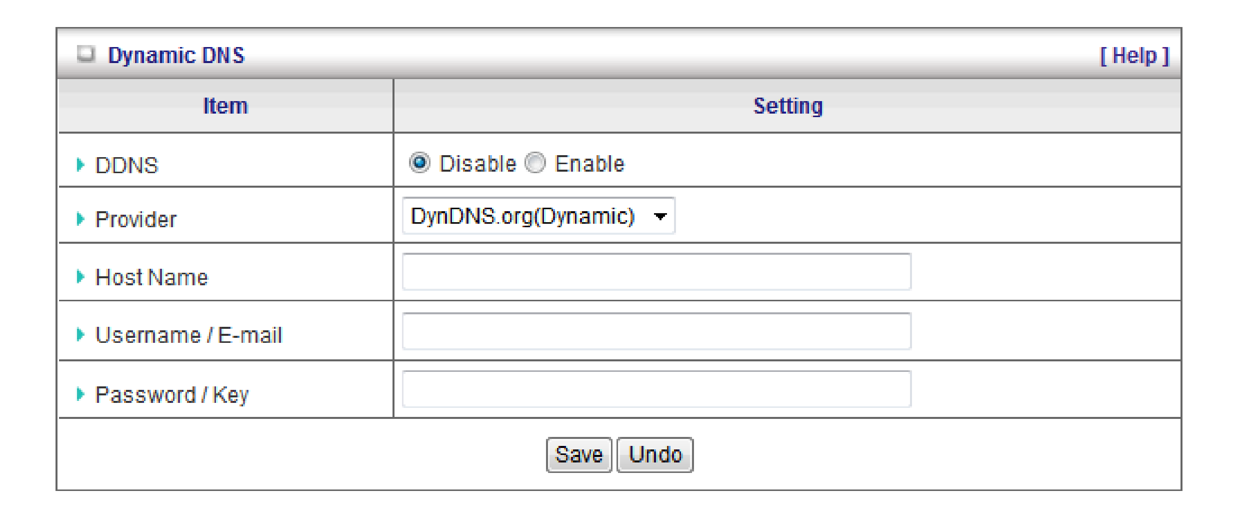
Für Syslog müssen Sie die IP-Adresse des Hostcomputers eingeben, der die Syslog-Mitteilungen empfängt, und das Kästchen **Enable (Aktivieren)** mit einem Häkchen versehen.

Für E-Mailwarnung müssen Sie Folgendes festlegen:

- **E-Mail Alert (E-Mailwarnung):** Versehen Sie das Kästchen **Enable (Aktivieren)** mit einem Häkchen, um diese Funktion zu aktivieren.
- **SMTP Server IP/Port (SMTP-Server-IP/Port):** Geben Sie die IP-Adresse und den Port des SMTP-Servers getrennt durch ":" ein. (Ohne Anführungszeichen). Wird keine Port-Nummer eingegeben, wird der Standardwert 25 verwendet.
- **SMTP User Name (SMTP-Benutzername) / SMTP Password (SMTP-Kennwort):** Geben Sie hier Ihren Benutzernamen und das Kennwort an, wenn Sie sich beim SMTP-Server anmelden müssen.
- **E-mail address (E-Mailadresse):** Geben Sie hier die E-Mailadressen der Empfänger für die E-Mailprotokolle ein. Um mehr als einen Empfänger zuzuweisen, trennen Sie die E-Mailadressen mit ";" oder "," (ohne Anführungszeichen).
- **E-Mail Subject (E-Mailbetreff):** Geben Sie den Betreff für die E-Mail (optional) ein.

Dynamic DNS (Dynamisches DNS)

Dynamic DNS (Dynamisches DNS) ist eine Funktion, die Benutzern die Einrichtung eines statischen Domänennamens gestattet, auch wenn sie eine dynamische Internet-IP-Adresse haben. Selbst wenn sich Ihre IP-Adresse bei jeder Verbindung mit dem Internet-Dienstanbieter ändern sollte, kann die IP-Adresse einem Hostnamen zugeordnet werden, so dass jeder, der sich mit dem WBR-6022 oder einem Dienst aus dem Internet hinter dem Router verbinden möchten, nur den dynamischen DNS-Hostnamen anstelle der änderbaren IP-Adresse einzugeben braucht.



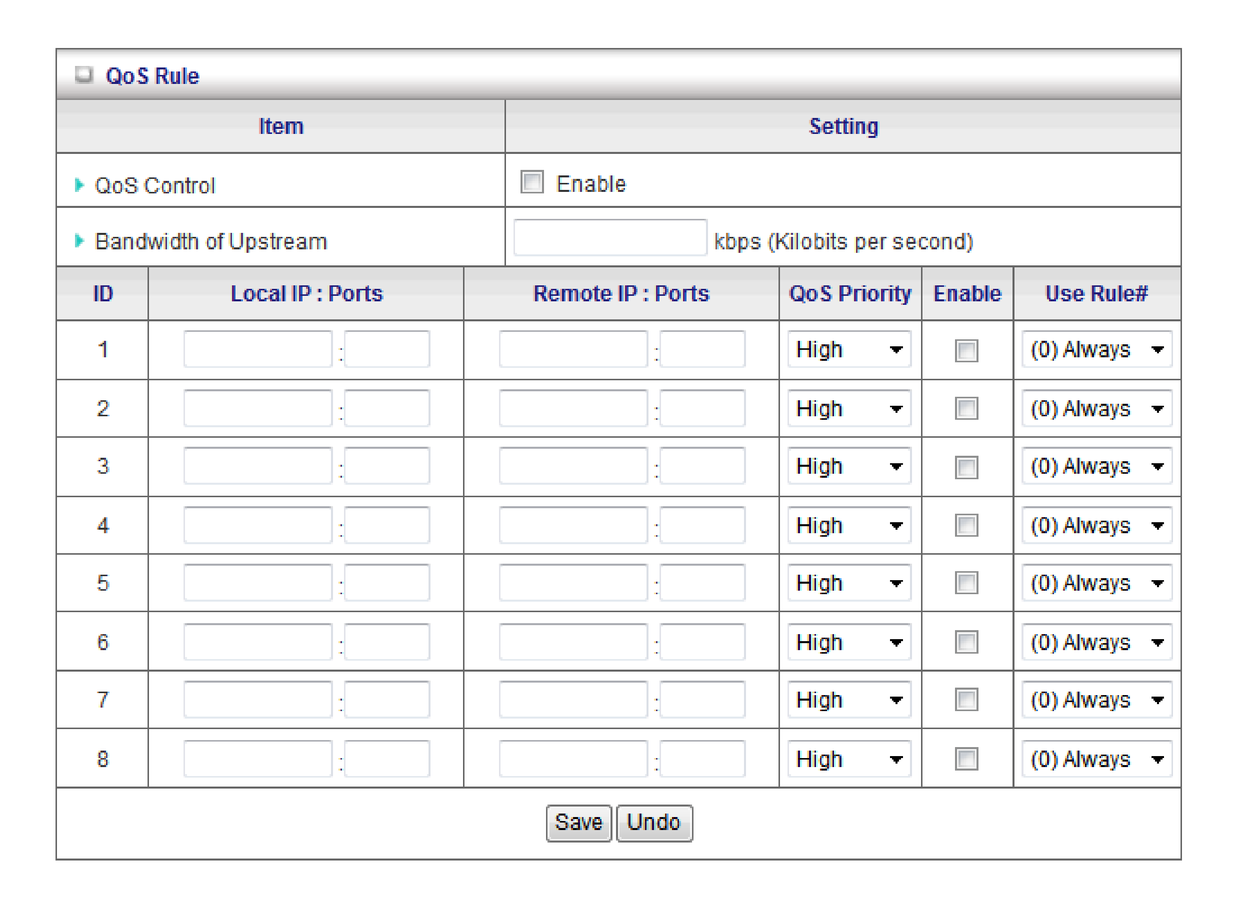
Bevor Sie **Dynamic DNS (Dynamisches DNS)** aktivieren, müssen Sie ein Konto bei einem der unterstützten “Provider” (Anbieter) für dynamisches DNS in der Liste registrieren. Nach erfolgreicher Registrierung des Kontos erhalten Sie vom Anbieter für dynamisches DNS die folgenden Details:

- Host Name (Hostname)
- Username/Email (Benutzername/E-Mail)
- Password (Kennwort)

Zur Aktivierung von Dynamic DNS (Dynamisches DNS) klicken Sie in das Kästchen “Enable” (Aktivieren) neben dem “DDNS”-Feld und wählen Sie den entsprechenden Anbieter für dynamisches DNS aus. Geben Sie gewünschten Details ein und klicken Sie auf **Save (Speichern)**, um die Einstellungen zu speichern, oder auf **Undo (Rückgängig)**, um sie zu ignorieren.

QoS Rule (QoS-Regel)

Hier können Sie die Parameter für QoS (Quality of Service, Dienstgüte) einstellen. Mit dieser Funktion können Sie angeben, welchen Typen von Datenpaketen Priorität gegeben wird. Sie können z.B. die Priorität von Voice Over IP- (IP-Telefonie) oder von Spiele-Paketen erhöhen, damit sie zuerst vom WBR-6022 verarbeitet werden.



Um den Punkt “QoS Control” (QoS-Kontrolle) zu aktivieren, versehen Sie das Kästchen **Enable (Aktivieren)** mit einem Häkchen.

Local IP (Lokales IP): Geben Sie hier das Client-IP ein, z.B.: 192.168.12.33. Dies ist der Computer, auf den sich die Regel bezieht.

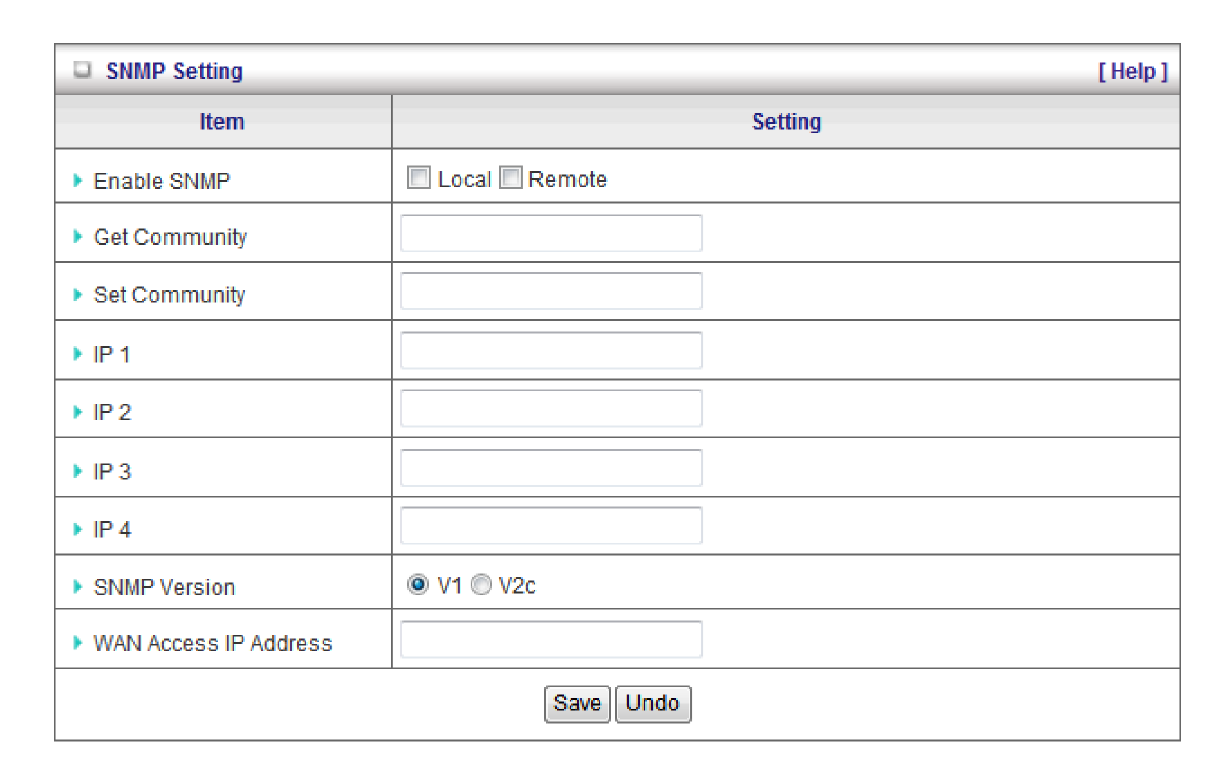
Remote IP (Ferngesteuertes IP): Geben Sie hier das globale IP und den Port ein, z.B.: 168.96.2.3 und Port 21. Auf diese Weise bezieht sich die QoS-Regel nur auf Pakete von dieser Internetquelle.

Priority (Priorität): Legen Sie fest, ob dieser bestimmten Regel die Priorität “High” (Hoch), “Normal” (Normal) oder “Low” (Niedrig) zugewiesen werden soll.

Use Rule # (Regelnr. verwenden): Legen Sie hier fest, welchem Zeitplan diese Regel folgen soll. Beispiel: Zu welchen Zeiten diese Regel angewandt wird.

SNMP Setting (SNMP-Einstellung)

SNMP (Simple Network Management Protocol, Einfaches Netzwerkverwaltungsprotokoll) versetzt Benutzer in die Lage, einen Computer oder ein Netzwerkgerät ferngesteuert zu verwalten.



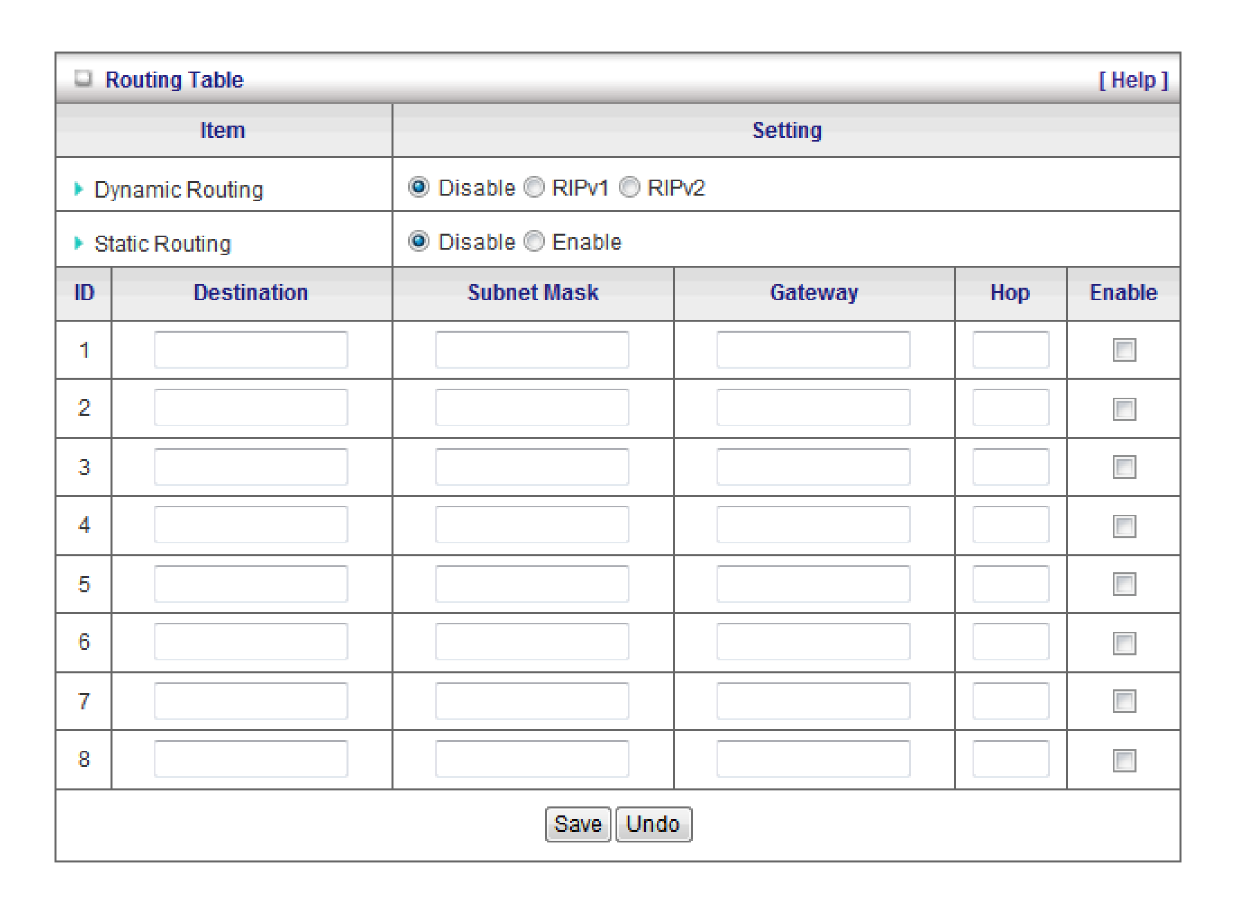
Zur Aktivierung von SNMP legen Sie bitte Folgendes fest:

- **Enable SNMP (SNMP aktivieren):** Sie müssen entweder “Local” (Lokalsteuerung) oder “Remote” (Fernsteuerung) oder beides mit einem Häkchen versehen, um die SNMP-Funktion zu aktivieren. Ist “Local” (Lokalsteuerung) abgehakt, reagiert dieses Gerät auf Anfragen vom LAN. Ist “Remote” (Fernsteuerung) abgehakt, reagiert dieses Gerät auf Anfragen vom WAN.
- **Get Community (Community beziehen):** Legt die Community von “GetRequest” (Anfrage beziehen) fest. Dies fungiert als ein Kennwort.
- **Set Community (Community einstellen):** Legt die Community von “SetRequest” (Anfrage einstellen) fest. Dies fungiert als ein Kennwort.
- **IP 1, IP 2, IP 3, IP 4:** Geben Sie hier die IP-Adressen der verwalteten PCs ein. Das Gerät sendet dann SNMP-Trap-Mitteilungen nur an die aufgelisteten IP-Adressen.
- **SNMP Version (SNMP-Version):** Wählen Sie hier die SNMP-Version Ihrer SNMP-Verwaltungssoftware.

Klicken Sie auf **Save (Speichern)**, um die Einstellungen zu speichern, oder auf **Undo (Rückgängig)**, um sie zu ignorieren.

Routing Table (Routingtabelle)

Wenn Sie mehr als einen WBR-6022 oder Router mit unterschiedlichen Subnetzen im Netzwerk besitzen, müssen Sie diese Funktion aktivieren, damit die unterschiedlichen Subnetze miteinander kommunizieren können.



Es gibt zwei Routingtypen, die vom WBR-6022 unterstützt werden.

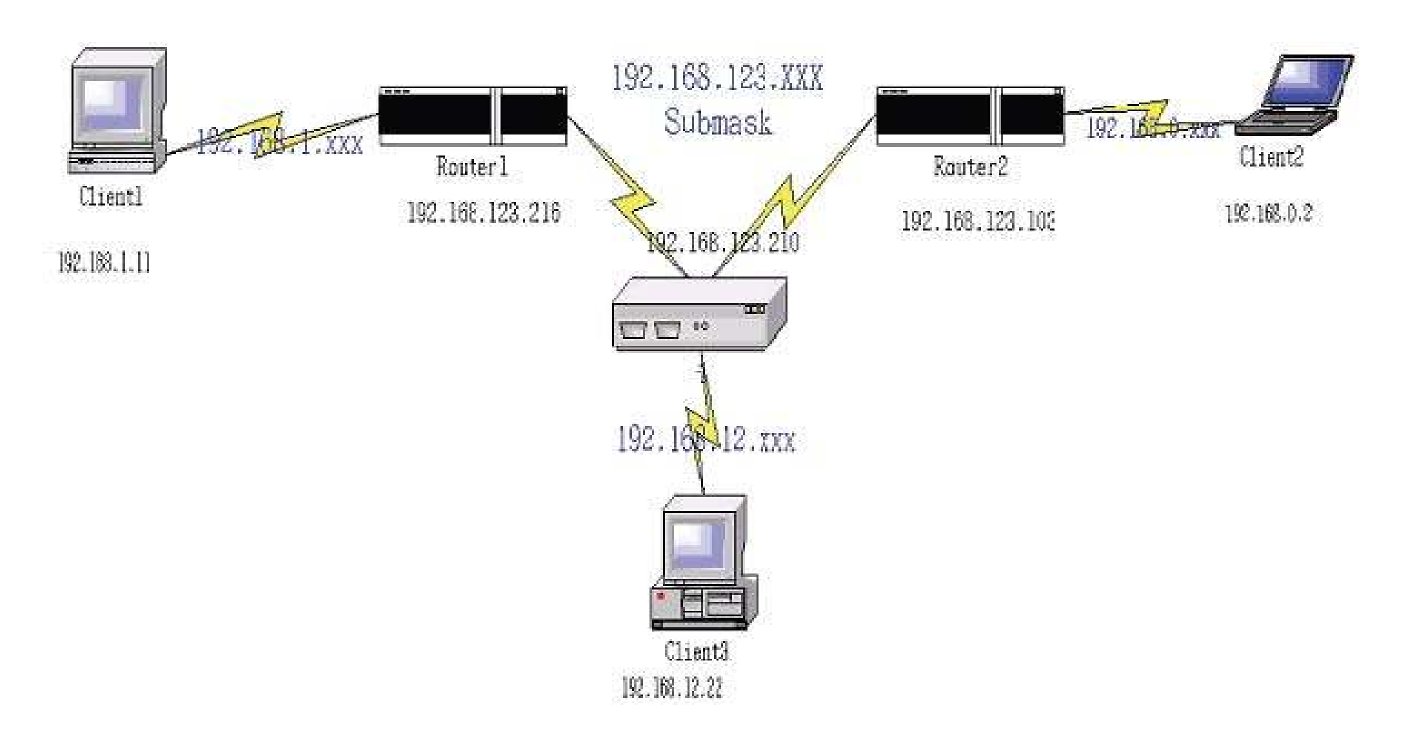
- **Dynamic Routing (Dynamisches Routing):** Diese Methode aktiviert die Geräte mit RIP (Routing Information Protocol, Routing-Informationsprotokoll), um die beste Route für jedes einzelne Paket anhand der Anzahl der Hops zwischen Quelle und Ziel zu ermitteln.

  Versehen Sie das Kästchen **Enable (Aktivieren)** mit einem Häkchen, um dynamisches Routing zu aktivieren. Verwenden Sie RIPv2 nur, wenn Sie unterschiedliche Subnetze in Ihrem Netzwerk haben. Andernfalls wählen Sie bitte RIPv1, sofern Sie dieses Protokoll benötigen.

- **Static Routing (Statisches Routing):** Hierbei können Computer, die mit dem WBR-6022 verbunden sind, mit Computern auf anderen LAN-Segmenten kommunizieren, die mit dem WBR-6022 über einen anderen Router verbunden sind. Sie können bis zu acht Routingregeln festlegen.

  Die nachstehenden Details sind für die Einstellung der Routingregeln erforderlich:

- IP-Adresse
- Subnetzmaske
- Gateway
- Hop, Anzahl der Hops
- Versehen Sie das Kästchen **Enable (Aktivieren)** jeder einzelnen Regel mit einem Häkchen.



Destination (Ziel)	Subnet Mask (Subnetzmaske)	Gateway (Gateway)	Hop (Hop)	Enable (Aktivieren)
192.168.1.0	255.255.255.0	192.168.123.216	1	✓
192.168.0.0	255.255.255.0	192.168.123.103	1	✓

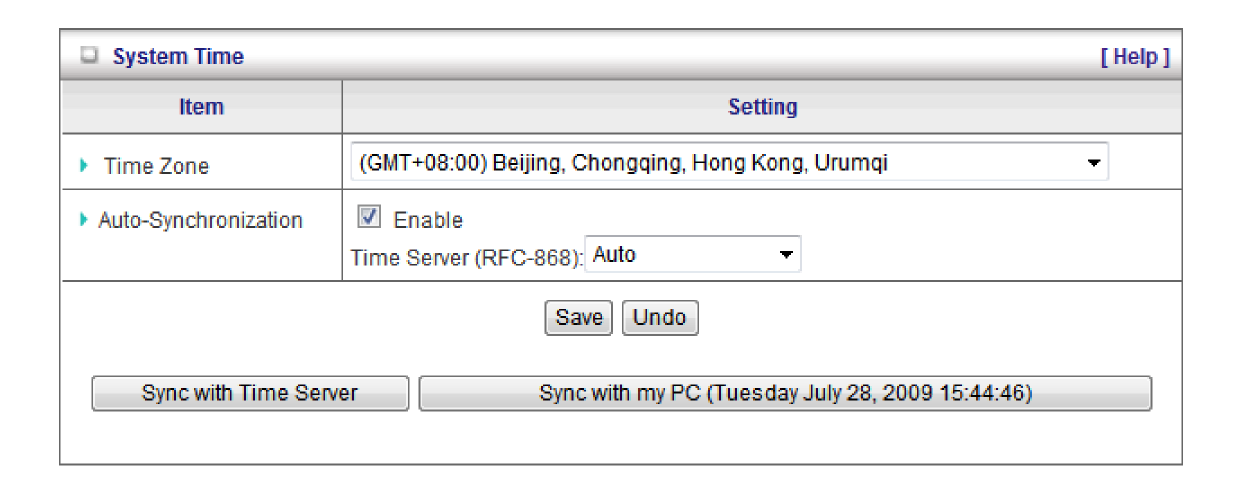
Möchte z.B. Client 3 ein IP-Datenpaket an 192.168.0.2 senden, würde er anhand der obigen Tabelle ermitteln, dass er über 192.168.123.103 (Router 2) zu gehen hat.

Und möchte er Pakete an 192.168.1.11 senden, wird er über 192.168.123.216 (Router 1) gehen. Jede Regel kann einzeln aktiviert oder deaktiviert werden.

Klicken Sie nach Konfiguration der Einstellung für **Routing Table (Routingtabelle)** auf die Schaltfläche **Save (Speichern)**.

System Time (Systemzeit)

Auf dieser Seite können Sie die Zeit für den WBR-6022 einstellen.



Time Zone (Zeitzone): Legen Sie die Zeitzone Ihres Standorts fest.

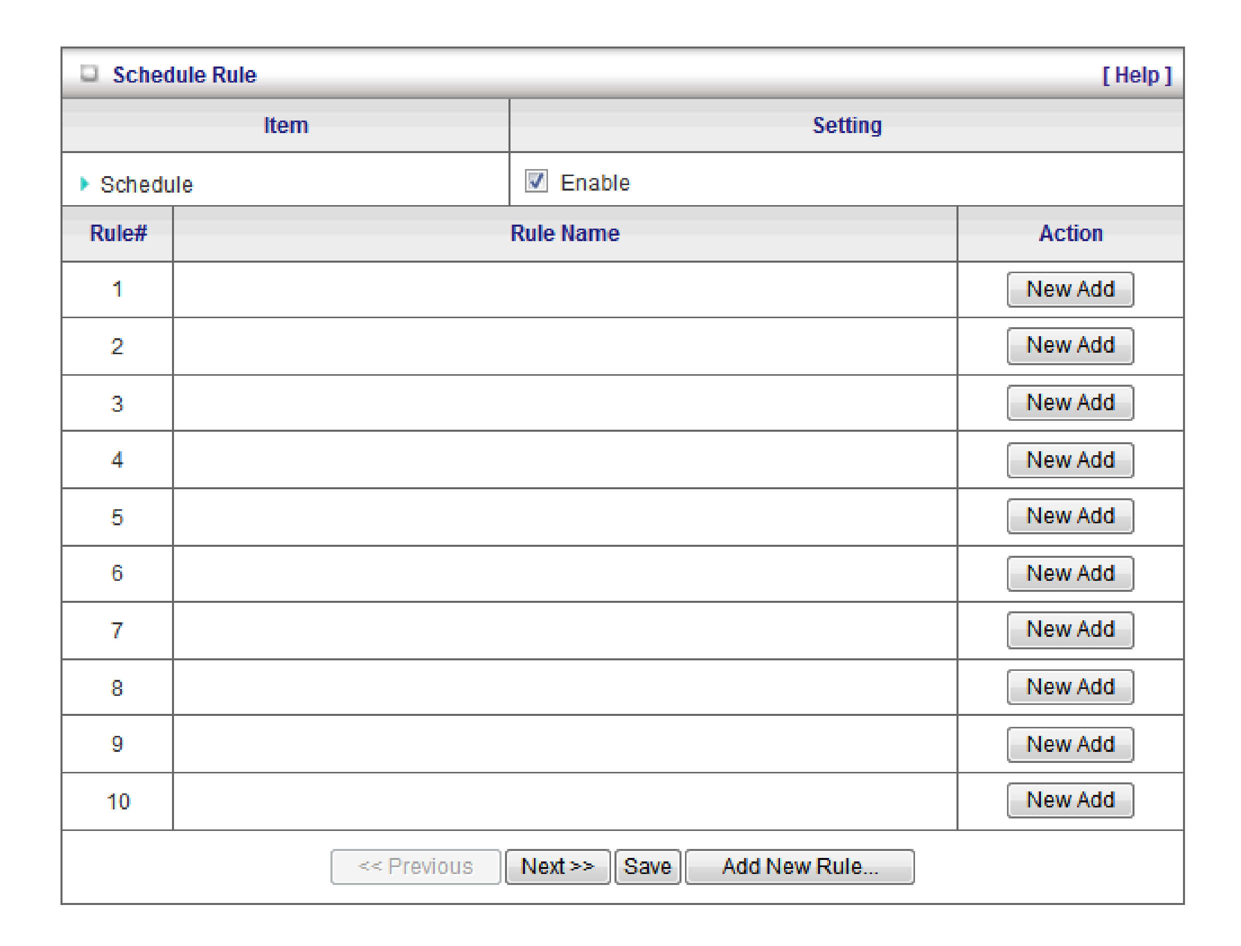
Auto-Synchronization (Autom. Synchronisierung): Der Router bleibt automatisch mit dem NTP-Zeitserver synchronisiert.

Sync with Time Server (Mit Zeitserver synchronisieren): Zwingt den Router, sich mit dem Zeitserver zu synchronisieren.

Sync with my PC (Mit meinem PC synchronisieren): Der Router verwendet die auf Ihrem Computer eingestellte Zeit.

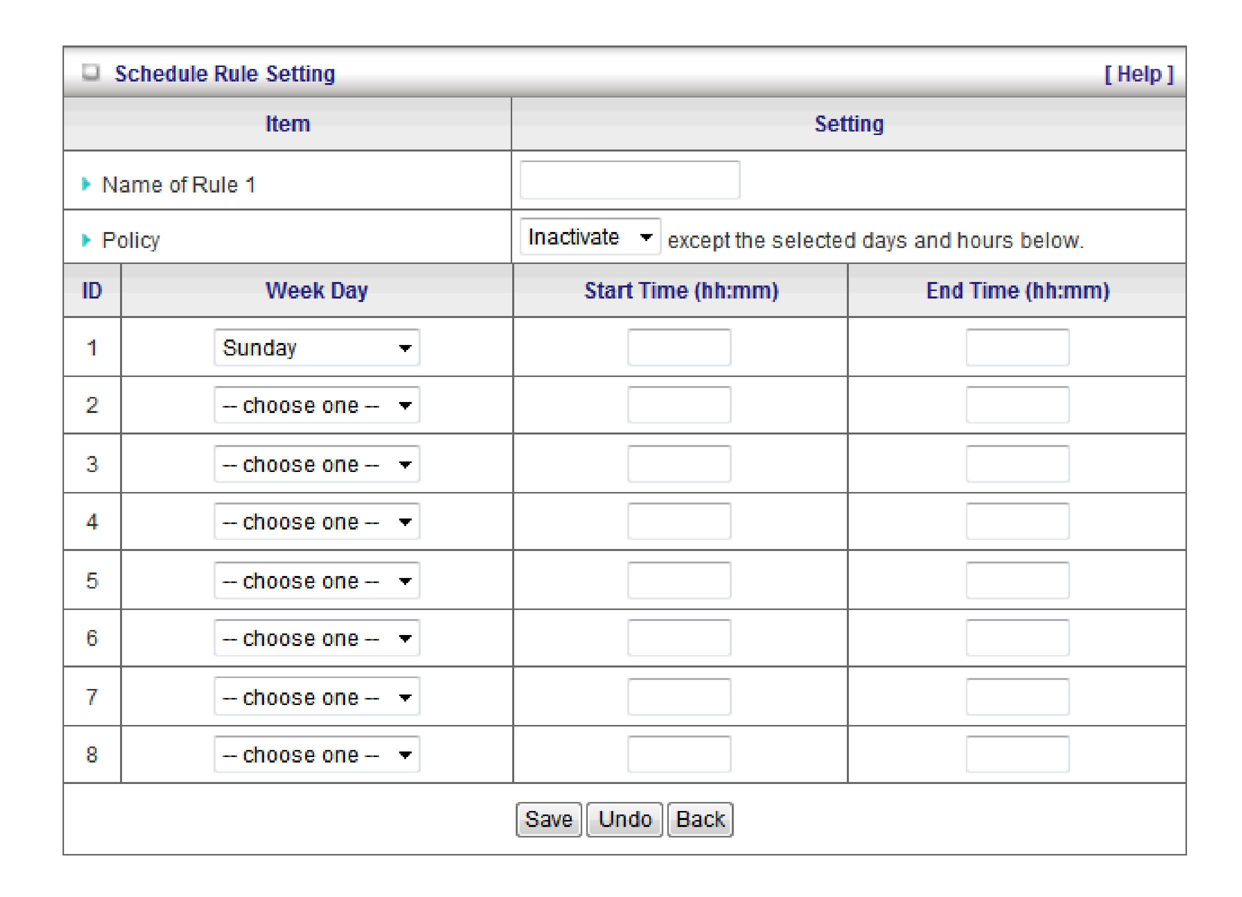
Schedule Rule (Regelzeit programmieren)

Mit dieser Funktion können Sie den Zeitplan der Regeln für den virtuellen Server und den Paketfilter festlegen.



Zur Aktivierung der Zeitprogrammierung versehen Sie das Kästchen **Enable (Aktivieren)** mit einem Häkchen und klicken Sie auf **Save (Speichern)**.

Erstellen Sie dann neue Regeln, indem Sie die Schaltfläche **New Add (Neu hinzufügen)** anklicken.

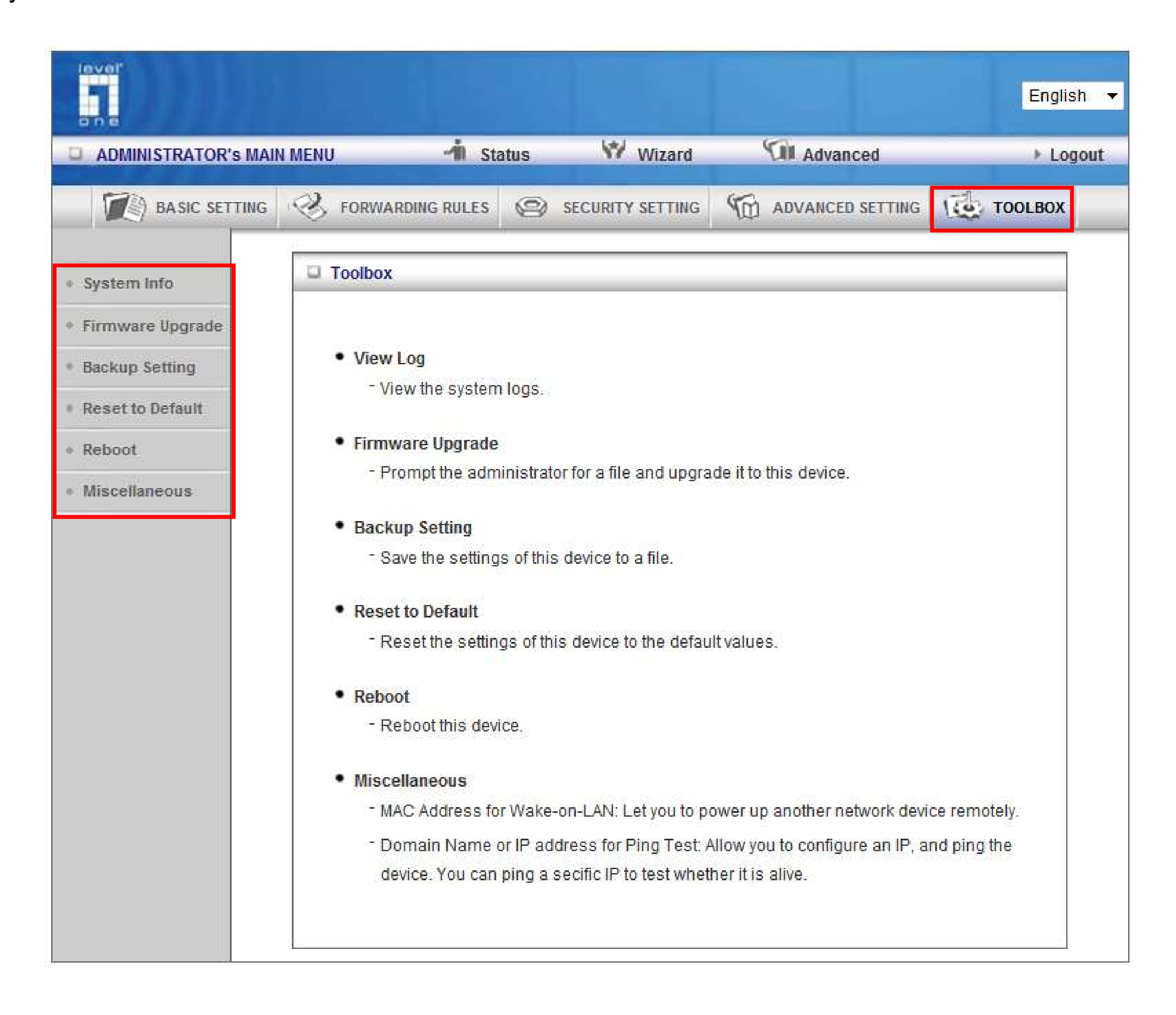


Geben Sie den Namen der Regel ein und legen Sie “Start Time” (Startzeit) und “End Time” (Endzeit) für jeden einzelnen Tag fest. Klicken Sie dann auf **Save (Speichern)**, um die neue Regel zu speichern.

Sobald die Regel festgelegt ist, können Sie sie für den virtuellen Server und Paketfilter verwenden, indem Sie die Regelnummer in den Feldern “Use Rule#” (Regelnr. verwenden) eingeben.

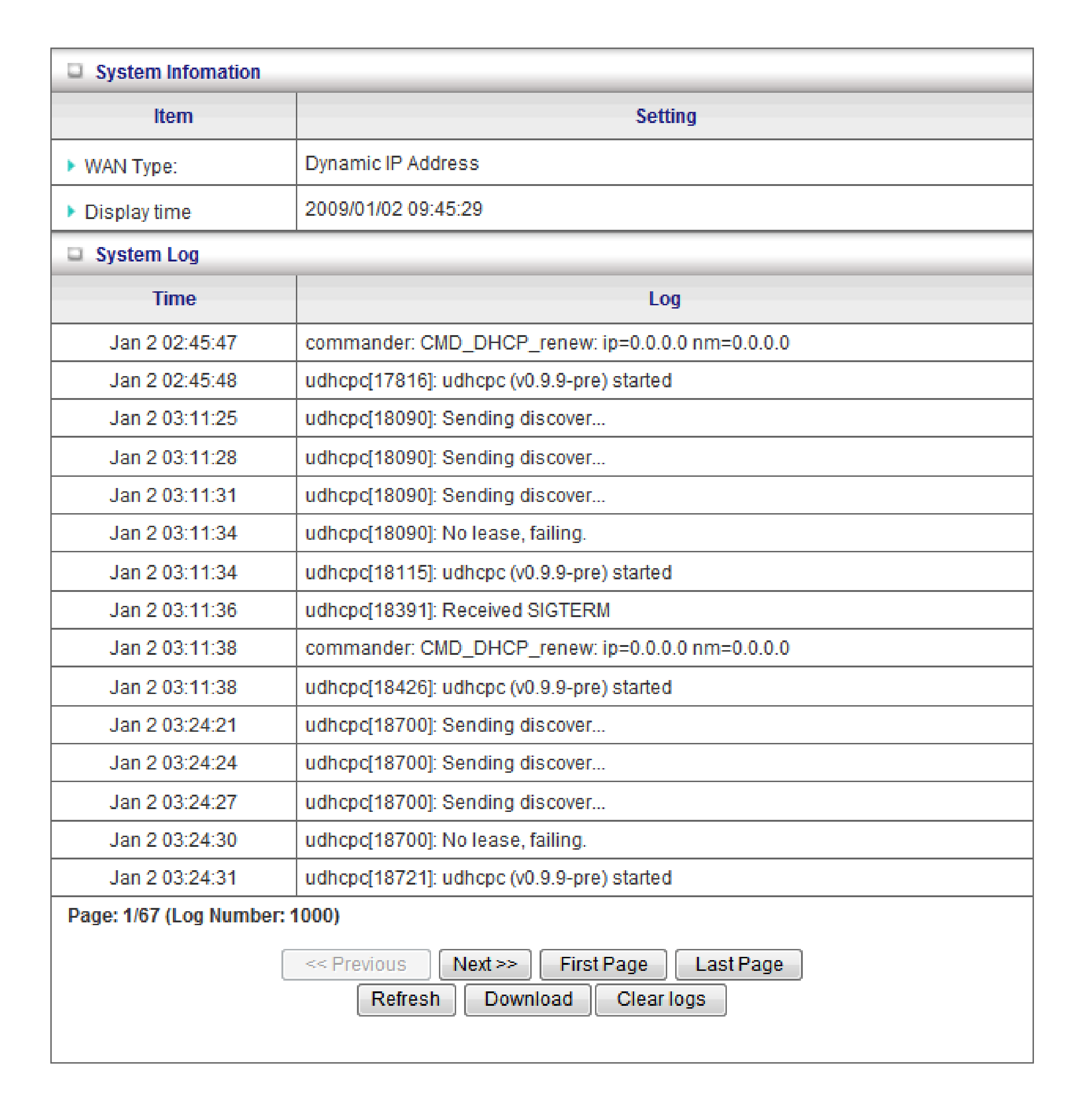
Toolbox (Toolbox)

In diesem Abschnitt befinden sich einige grundlegende Werkzeuge zur Wartung des WBR-6022-Systems.



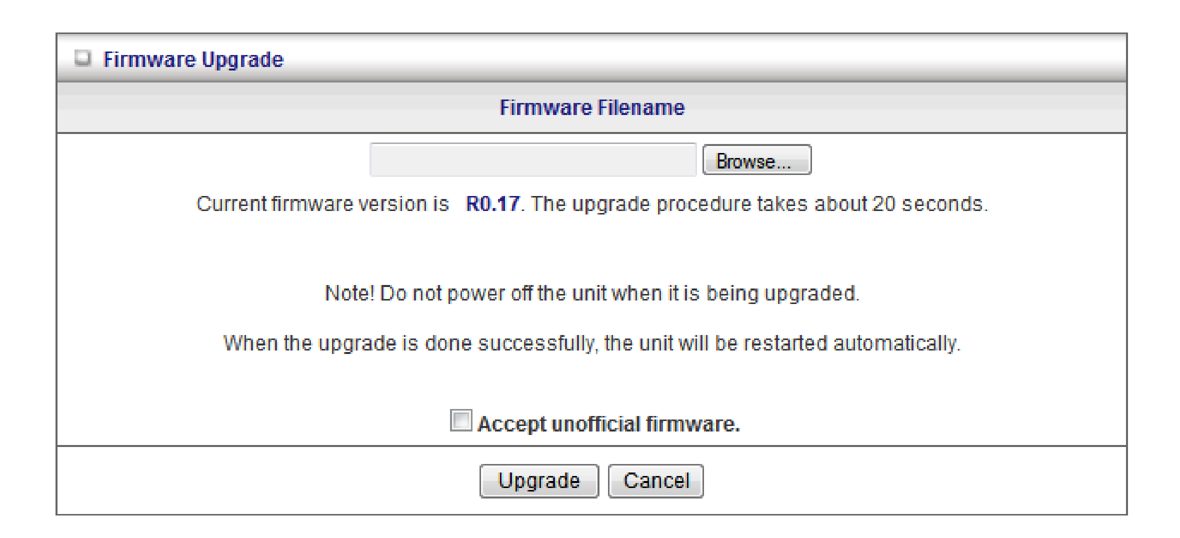
System Information (Systeminformationen)

Zeigt das Protokoll des Routers an. Es kann auch als Textdatei exportiert werden.



Firmware Upgrade (Firmware-Aktualisierung)

Auf dieser Seite können Sie die Firmware für den WBR-6022 aktualisieren.



Klicken Sie zu diesem Zweck auf **Browse (Durchsuchen)** und suchen Sie die Abbilddatei der Firmware; klicken Sie dann auf **Upgrade (Aktualisieren)**.

Hinweis: Schließen Sie für diesen Vorgang den WBR-6022 mit einer Drahtverbindung an das LAN an, denn wenn die Verbindung während der Aktualisierung unterbrochen wird, funktioniert das Gerät nicht mehr. Deaktivieren Sie auch Virenscanner oder Firewall-Programme, bevor Sie mit der Aktualisierung beginnen.

Accept unofficial firmware (Inoffizielle Firmware akzeptieren): Zwingt den Router, inoffizielle Firmware-Dateien zu akzeptieren. LevelOne empfiehlt, diese Funktion NICHT zu verwenden.

Backup Setting (Sicherungseinstellung)

Sie können Ihre Einstellungen absichern, indem Sie die Schaltfläche **Backup Setting (Sicherungseinstellung)** anklicken und die gesicherten Daten als Bin-Datei abspeichern. Wenn Sie diese Einstellungen eines Tages wiederherstellen möchten, klicken Sie auf die Schaltfläche **Firmware Upgrade (Firmware-Aktualisierung)** und verwenden Sie die gespeicherte Bin-Datei.

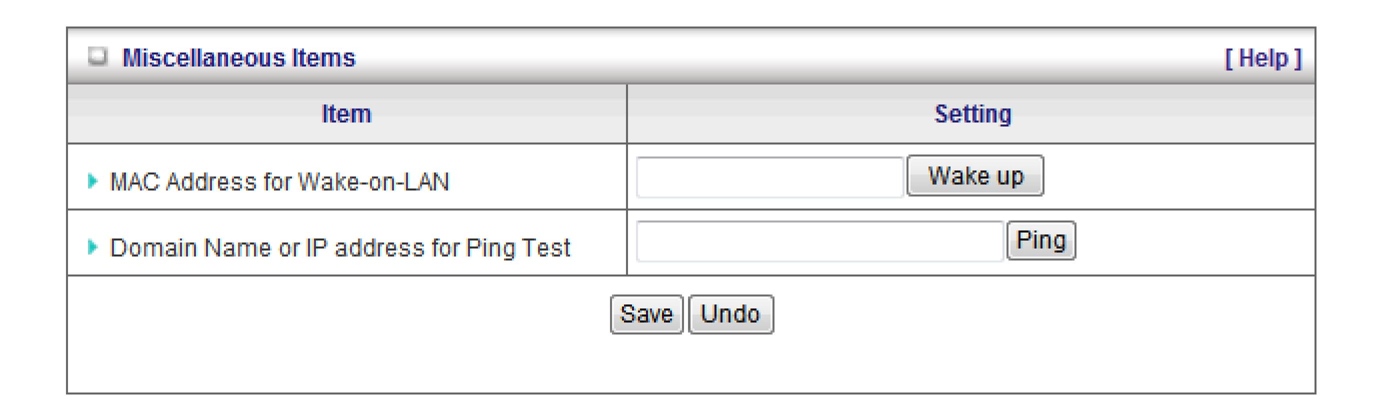
Reset to default (Auf Standard zurücksetzen)

Sie können das Gerät auch wieder auf die werseitigen Standardeinstellungen zurücksetzen, indem Sie die Schaltfläche **Reset to Default (Auf Standard zurücksetzen)** und dann OK anklicken. Warten Sie, bis das Gerät neu startet.

Reboot (Neustart)

Um das Gerät manuell neu zu starten, klicken Sie auf die Schaltfläche **Reboot (Neustart)** und dann auf OK.

Miscellaneous Items (Verschiedenes)



MAC Address for Wake-on-LAN (MAC-Adresse für ferngesteuerte Aktivierung über LAN)
Wake-on-LAN ist eine Technologie, mit der Sie ein Netzwerkgerät per Fernsteuerung aktivieren können. Um diese Funktion nutzen zu können, muss Wake-on-LAN auf dem Zielgerät aktiviert sein und Sie müssen die MAC-Adresse dieses Geräts kennen, z.B. 00-11-22-33-44-55. Wenn Sie die Schaltfläche "Wake up" (Systemaktivierung) anklicken, sendet der Router sofort das Aktivierungssignal an das Zielgerät.

Domain Name or IP Address for Test (Domänenname oder IP-Adresse für Test)
Hier können Sie ein IP konfigurieren und das Gerät pingen. Sie können ein bestimmtes IP pingen, um zu testen, ob es aktiv ist.

Anhang A 802.1x Einstellung

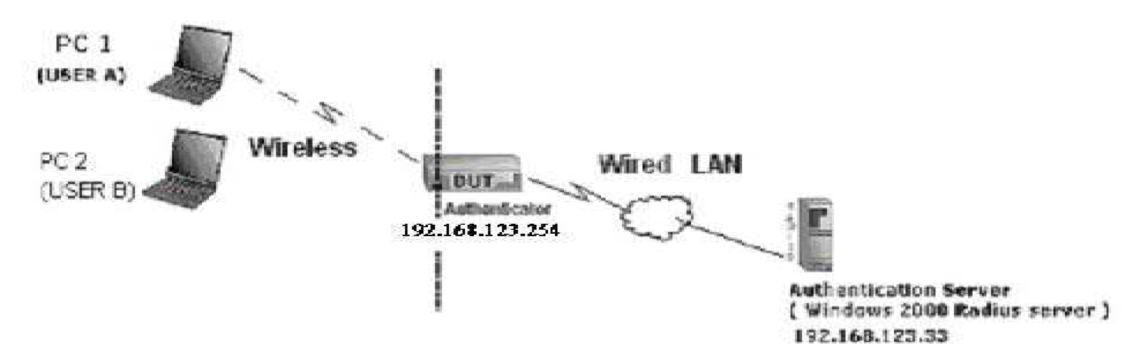


Abbildung 1: Testumgebung (Verwendung von Windows 2000 Radius-Server)

Details zu den Geräten

PC1: Microsoft Windows XP Professional ohne Service Pack 1 und LevelOne Wireless PCI-Karte.

PC2: Microsoft Windows XP Professional mit Service Pack 1a oder neuerer Version und LevelOne Wireless PCI-Karte.

Authentifizierungsserver: Windows 2000 RADIUS-Server mit Service Pack 3 und HotFix Q313664.



Hinweis: Windows 2000 RADIUS-Server unterstützt nur PEAP nach Upgrade auf Service Pack 3 und HotFix Q313664 *(weitere Informationen finden Sie unter http://support.microsoft.com/default.aspx?scid=kb; en-us;313664)*

DUT-Konfiguration für den Test:

1. DHCP-Server aktivieren.
2. WAN-Einstellung: Statische IP-Adresse.
3. LAN-IP-Adresse: 192.168.123.254/24.
4. RADIUS-Server-IP einstellen.
5. Freigabeschlüssel für RADIUS-Server einstellen.
6. WEP-Schlüssel und 802.1X-Einstellung konfigurieren.

Der folgende Test bedient sich der integrierten 802.1X-Authentifizierungsmethode wie EAP_TLS, PEAP_CHAPv2 (Windows XP nur mit SP1) sowie PEAP_TLS (Windows XP nur mit SP1) mit Smartcard oder ein anderes Zertifikat von Windows XP Professional.

DUT (Device under Test, Getestetes Gerät) und Einrichtung des Windows 2000 Radius-Servers

Richten Sie den Windows 2000 RADIUS-Server ein.

Wir müssen die Authentifizierungsmethode auf MD5_Challenge abändern oder Smartcard oder ein anderes Zertifikat auf dem RADIUS-Server entsprechend der Testbedingung verwenden.

Einrichten des DUT-Tests

1. Aktivieren Sie 802.1X (“Enable checkbox“ (Kästchen Aktivieren) abhaken).
2. Geben Sie die RADIUS-Server-IP ein.
3. Geben Sie den Freigabeschlüssel ein. (Der Schlüssel, der vom RADIUS-Server und dem DUT-Test gemeinsam verwendet wird.)
4. Wir ändern die Länge des 802.1X-Verschlüsselungsschlüssels, um sie den unterschiedlichen Testbedingungen anzupassen.

Einrichten der Netzwerkkarte auf dem PC

1. Wählen Sie IEEE802.1X als Authentifizierungsmethode. (Abb. 2)
2. Wählen Sie MD5-Challenge oder Smartcard oder ein anderes Zertifikat als EAP-Typ.
3. Bei Wahl von Smartcard oder des Zertifikats als EAP-Typ Zertificate verwenden wir ein Zertifikat auf diesem Computer.
4. Wir ändern den EAP-Typ, um ihn den unterschiedlichen Testbedingungen anzupassen.



Abbildung 2 zeigt die Einstellung von Windows XP ohne Service Pack 1. Nachdem Benutzer auf Service Pack 1 aufgerüstet haben, ist MD5-Challenge in der EAP-Typenliste nicht mehr zu sehen, aber es erscheint eine neue Option namens “Protected EAP” (PEAP, Geschütztes EAP).

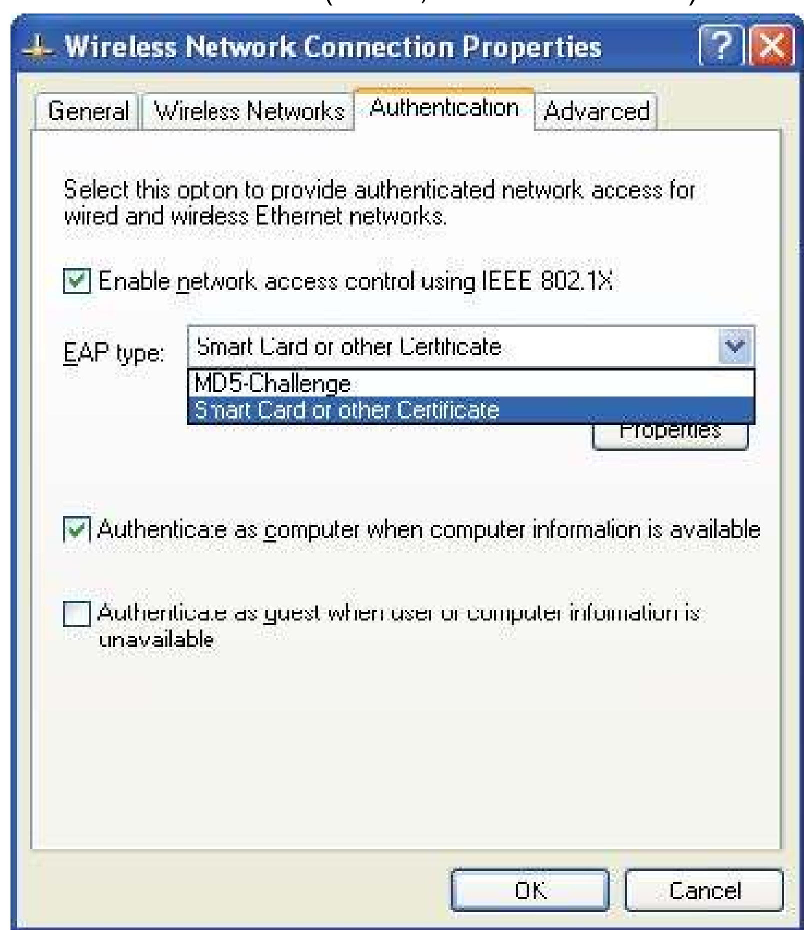


Abbildung 2: Aktivierung der Eigenschaften von IEEE 802.1X-Zugangskontrolle / Smartcard oder Zertifikat

Testen der Authentifizierung von Windows 2000 RADIUS-Server:

DUT-Authentifizierung von PC1 mit Zertifikat. (PC2 folgt demselben Testverfahren.)

1. Laden Sie das Zertifikat auf PC1 herunter und installieren Sie es dort. (Abb. 4)
2. PC1 wählt die SSID vom DUT als Zugangspunkt (AP).
3. Setzen den Authentifizierungstyp vom Drahtlos-Client und vom RADIUS-Server auf EAP_TLS.
4. Deaktivieren Sie die Drahtlosverbindung und aktivieren Sie sie wieder.
5. DUT sendet dem RADIUS-Server das Benutzerzertifikat und meldet dann dem PC1 das Authentifizierungsergebnis. (Abb. 5)
6. Windows XP zeigt an, ob die Authentifizierung erfolgreich war oder fehlgeschlagen ist, und beendet den Authentifizierungsvorgang. (Abb. 6)
7. Brechen Sie die Testschritte ab, wenn PC1 ein dynamisches IP bezieht und ein PING erfolgreich zum ferngesteuerten Host gesendet wurde.

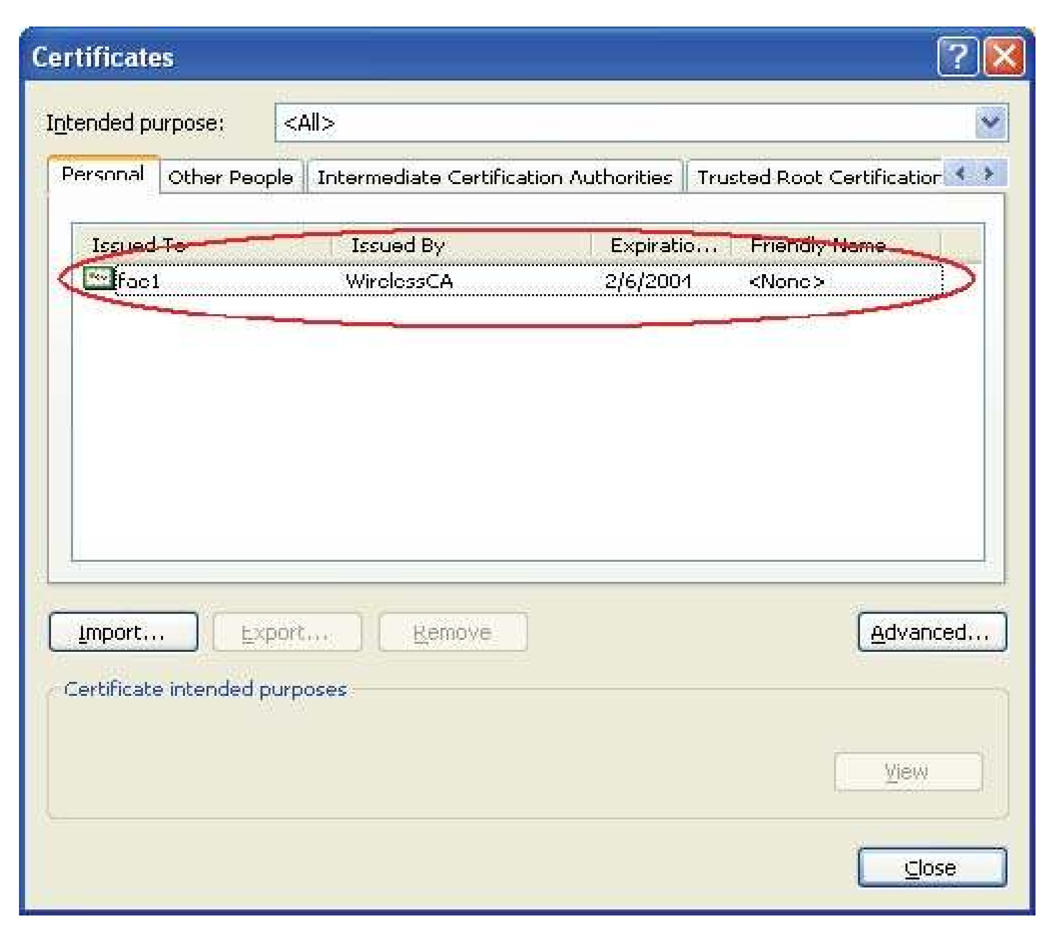


Abbildung 4: Zertifikatsinformationen auf PC1

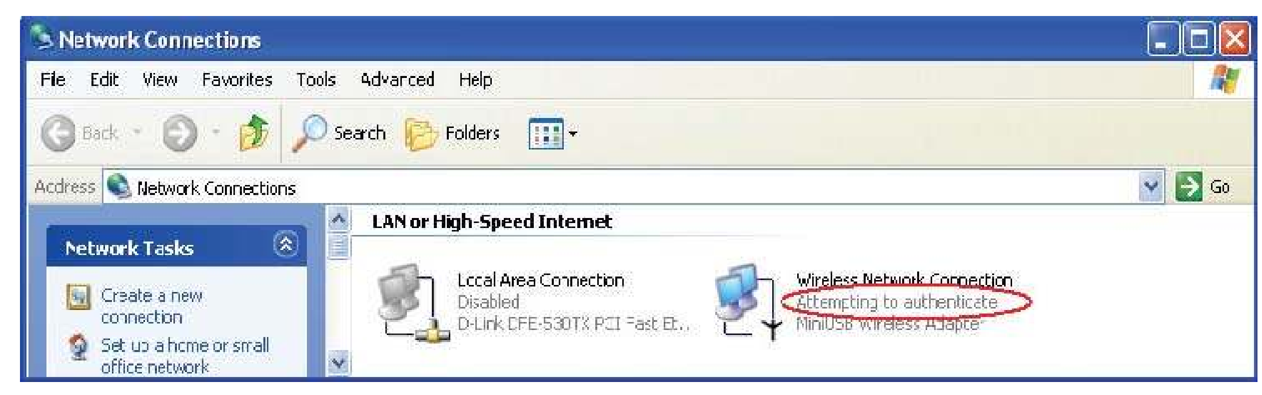


Abbildung 5: Authentifizierung

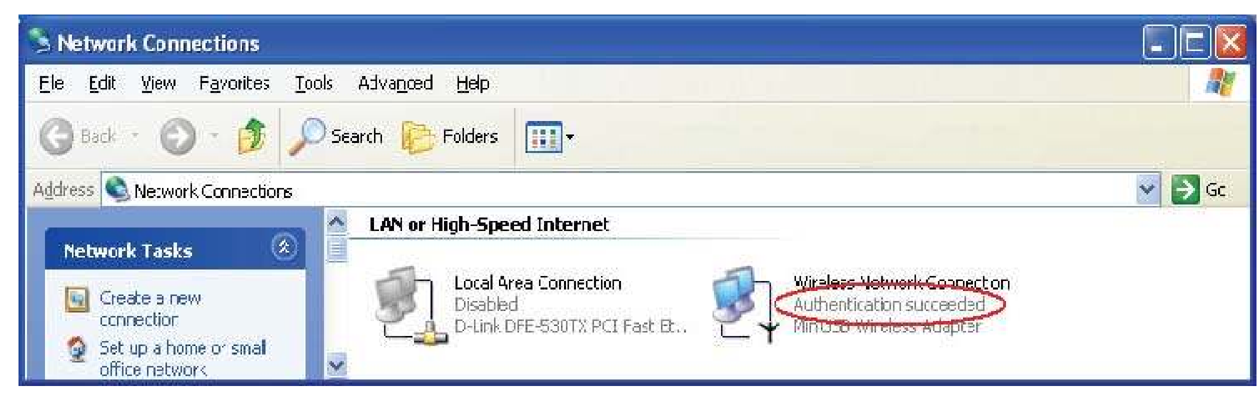


Abbildung 6: Authentifizierung erfolgreich

DUT-Authentifizierung von PC2 mit PEAP-TLS.

1. PC2 wählt die SSID vom DUT als Zugangspunkt (AP).
2. Setzen den Authentifizierungstyp vom Drahtlos-Client und vom RADIUS-Server auf PEAP_TLS.
3. Deaktivieren Sie die Drahtlosverbindung und aktivieren Sie sie wieder.
4. DUT sendet dem RADIUS-Server das Benutzerzertifikat und meldet dann dem PC2 das Authentifizierungsergebnis.
5. Windows XP zeigt an, ob die Authentifizierung erfolgreich war oder fehlgeschlagen ist, und beendet den Authentifizierungsvorgang.
6. Brechen Sie die Testschritte ab, wenn PC2 ein dynamisches IP bezieht und ein PING erfolgreich zum ferngesteuerten Host gesendet wurde.

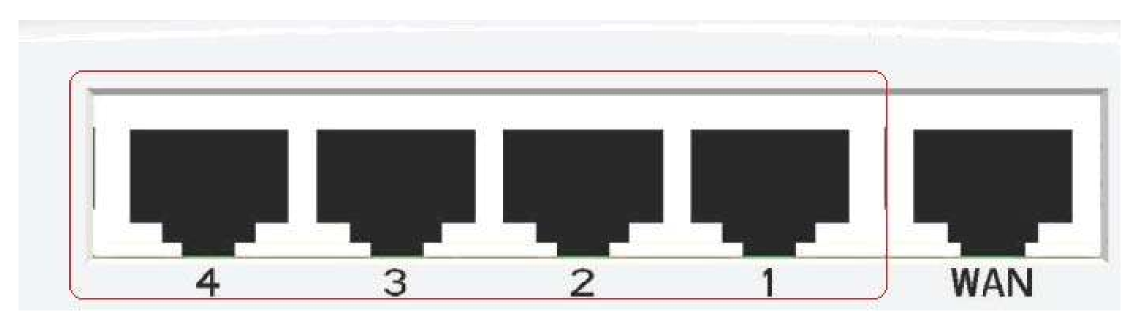
Unterstützte Typen: Der Router unterstützt folgende Typen der 802.1x-Authentifizierung: PEAP-CHAPv2 und PEAP-TLS.

Anhang B Häufig gestellte Fragen und Fehlerbehebung

Was kann ich tun, wenn gleich am Anfang Probleme auftreten?

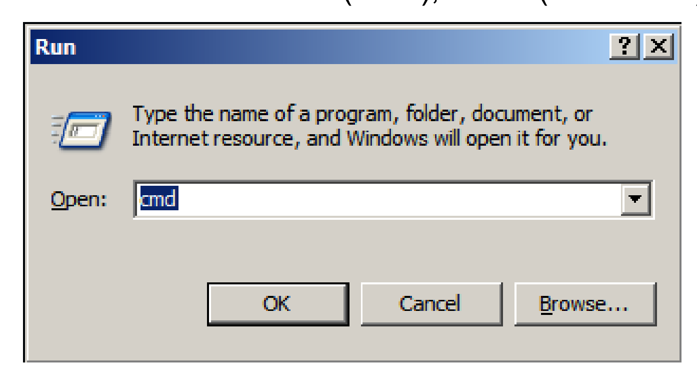
1. **Warum kann ich den Router nicht konfigurieren, selbst wenn Kabel mit den Router-Ports verbunden sind und sogar die LED leuchtet?**

A: Überprüfen Sie zuerst, welcher Port angeschlossen ist. Befindet sich das Kabel am WAN-Port, stecken Sie es bitte um auf LAN-Port 1 oder LAN-Port 4:



Prüfen Sie dann, ob Ihr PC eine IP-Adresse vom Router beziehen kann.

Klicken Sie auf “Start” (Start), “Run” (Ausführen).



Geben Sie **CMD** ein und klicken Sie auf “OK”.

Geben Sie bei der Befehlseingabe **ipconfig** ein, siehe unten.

```
Connection-specific DNS Suffix  . :
IP Address. . . . . . . . . . . . : 192.168.0.169
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.0.1
```

Wenn Sie sehen, dass Ihr PC eine IP-Adresse hat, öffnen Sie Ihren Webbrowser und geben Sie 192.168.0.1 in der Adressleiste ein.

Andernfalls geben Sie erst **ipconfig /release**, dann **ipconfig /renew** ein, um Ihre IP-Adresse zu aktualisieren.

2. Warum kann ich den Router nicht verbinden, selbst wenn ein Kabel mit dem LAN-Port verbunden ist und sogar die LED leuchtet?

A: Prüfen Sie zuerst die Status-LED. Ist der Gerätebetrieb normal, blinkt die LED einmal pro Sekunde.

Andernfalls prüfen Sie bitte die folgenden Blinksignale der Status-LED:

Status-LED ist durchgehend ein- oder ausgeschaltet:

Das System ist stehengeblieben. Schalten Sie den Router aus und dann wieder ein. Ändert sich hierdurch nichts, setzen Sie das Gerät auf seine Standardeinstellungen zurück oder aktualisieren Sie die Firmware auf die neueste Version und wiederholen Sie den Vorgang.

Status-LED blinkt unregelmäßig:

Es gibt einen Fehler im System. Setzen Sie das Gerät auf seine Standardeinstellungen zurück oder starten Sie den Router neu.

3. **Wie wird das Gerät auf die werkseitigen Standardeinstellungen zurückgesetzt?**

A: Hierfür gibt es 2 Methoden.

Methode 1) Wiederherstellung mit RESET-Taste (WLAN- und WPS-Taste gleichzeitig drücken)

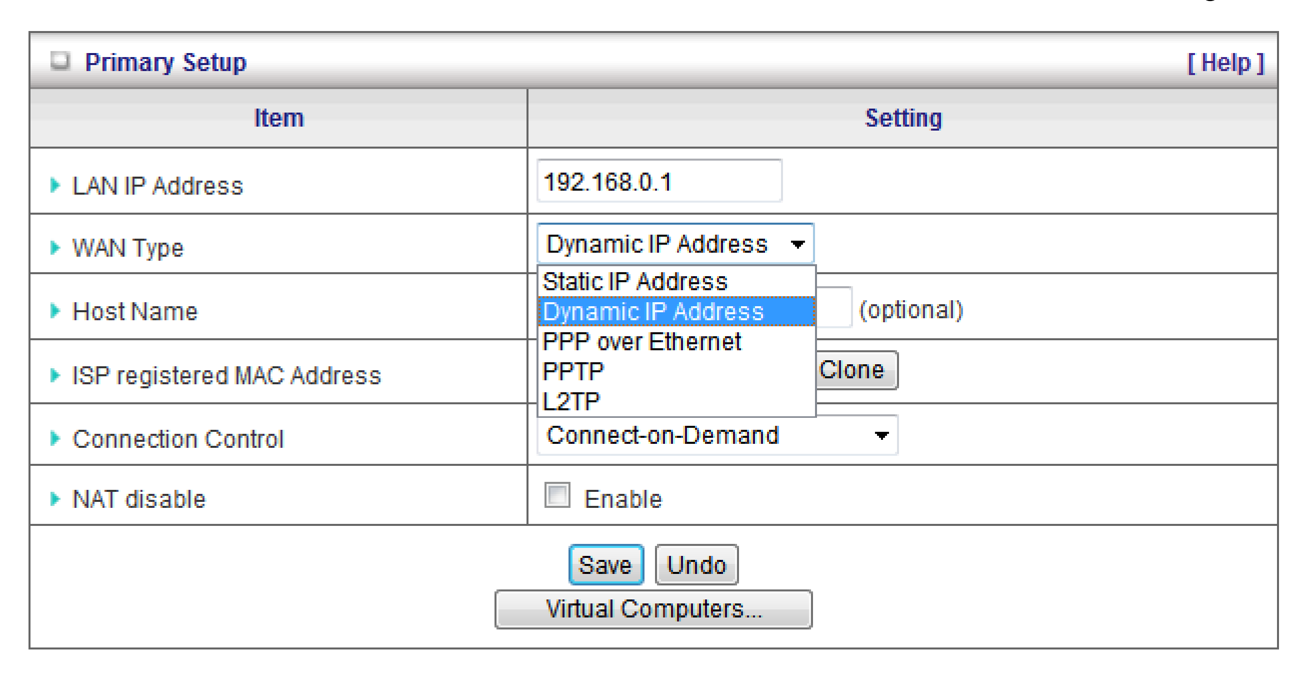
Schalten Sie zuerst den Router aus. Drücken Sie dann gleichzeitig die Tasten WLAN und WPS und schalten Sie den Router ein. Halten Sie diese Tastenkombination gedrückt, bis die Status-LED anfängt zu blinken; erst dann können Sie die Tasten wieder loslassen. Wenn die Status-LED etwa 8-mal blinkt, ist die WIEDERHERSTELLUNG abgeschlossen. Blinkt die LED jedoch nur 2-mal, wiederholen Sie bitte die obigen Schritte.

Methode 2) Direkte Wiederherstellung bei eingeschaltetem Router

Halten Sie die Tasten WLAN und WPS etwa 5 Sekunden lang gedrückt (Status-LED blinkt ca. 5-mal) und lassen Sie dann die Tasten wieder los. Die WIEDERHERSTELLUNG ist abgeschlossen.

4. **Warum kann ich mich nicht mit dem Internet verbinden, selbst wenn Kabel mit dem WAN- und LAN-Port verbunden sind und sogar die LEDs leuchten? Zudem leuchtet die Status-LED ganz normal, aber ich kann die Webverwaltung nicht konfigurieren.**

A: Vergewissern Sie sich, dass das Netzwerkkabel vom DSL- oder Kabelmodem mit dem WAN-Port des Routers und das Netzwerkkabel vom LAN-Port des Routers mit dem Ethernetadapter verbunden ist. Prüfen Sie dann, welchen WAN-Typ Sie verwenden. Sind Sie sich da nicht sicher, erkunden Sie sich bitte bei Ihrem Internet-Dienstanbieter. Rufen Sie dann bitte diese Seite auf, um die Informationen, die Sie von Ihrem Internet-Dienstanbieter erhalten haben, hier einzugeben.



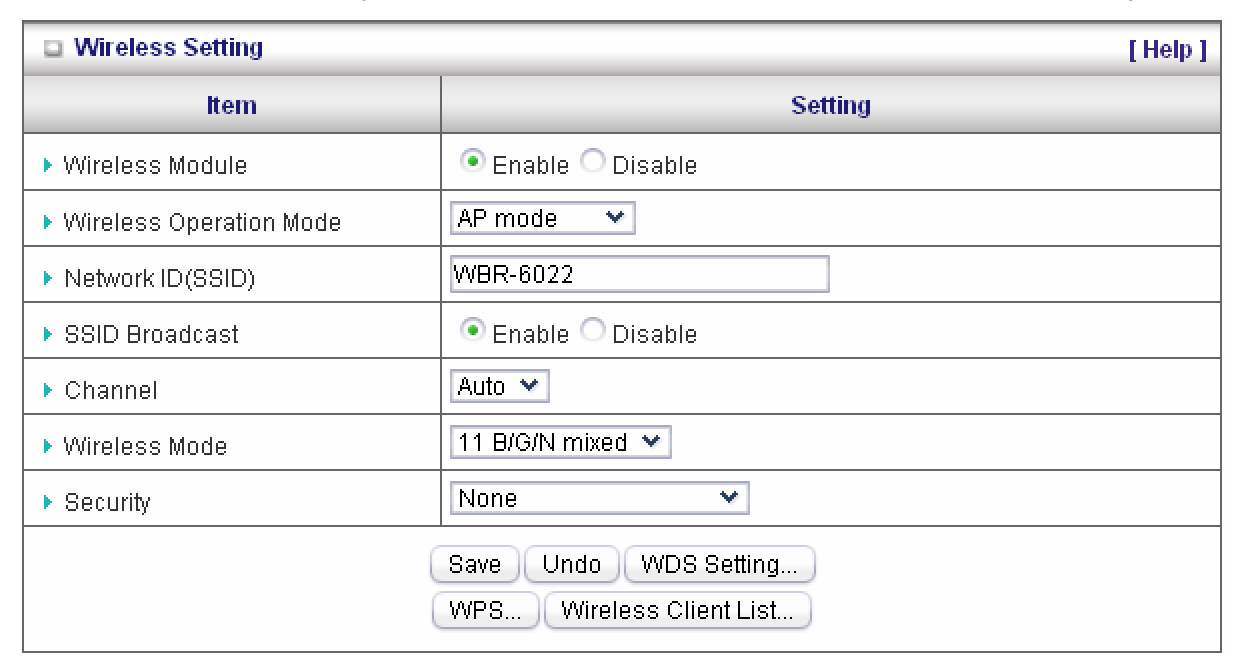
5. **Wenn ich mich mit einer statischen IP-Adresse mit dem Internet verbinden, kann ich auf globale IP-Adressen wie 202.93.91.218 zugreifen und ihnen ein Ping senden. Ich kann jedoch keine Website über ihren Domänennamen aufrufen, z.B. http://espn.com.**

A: Prüfen Sie die DNS-Konfiguration der statischen IP-Adresse. Halten Sie sich bitte an die Informationen vom Internet-Dienstanbieter und weisen Sie einen oder zwei DNS-Server zu.

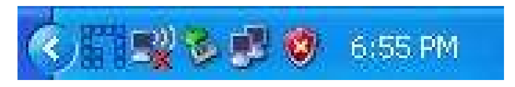
Wie verbinde ich den Router auf drahtlose Weise?

1. Wie starte ich die Drahtlosfunktion?

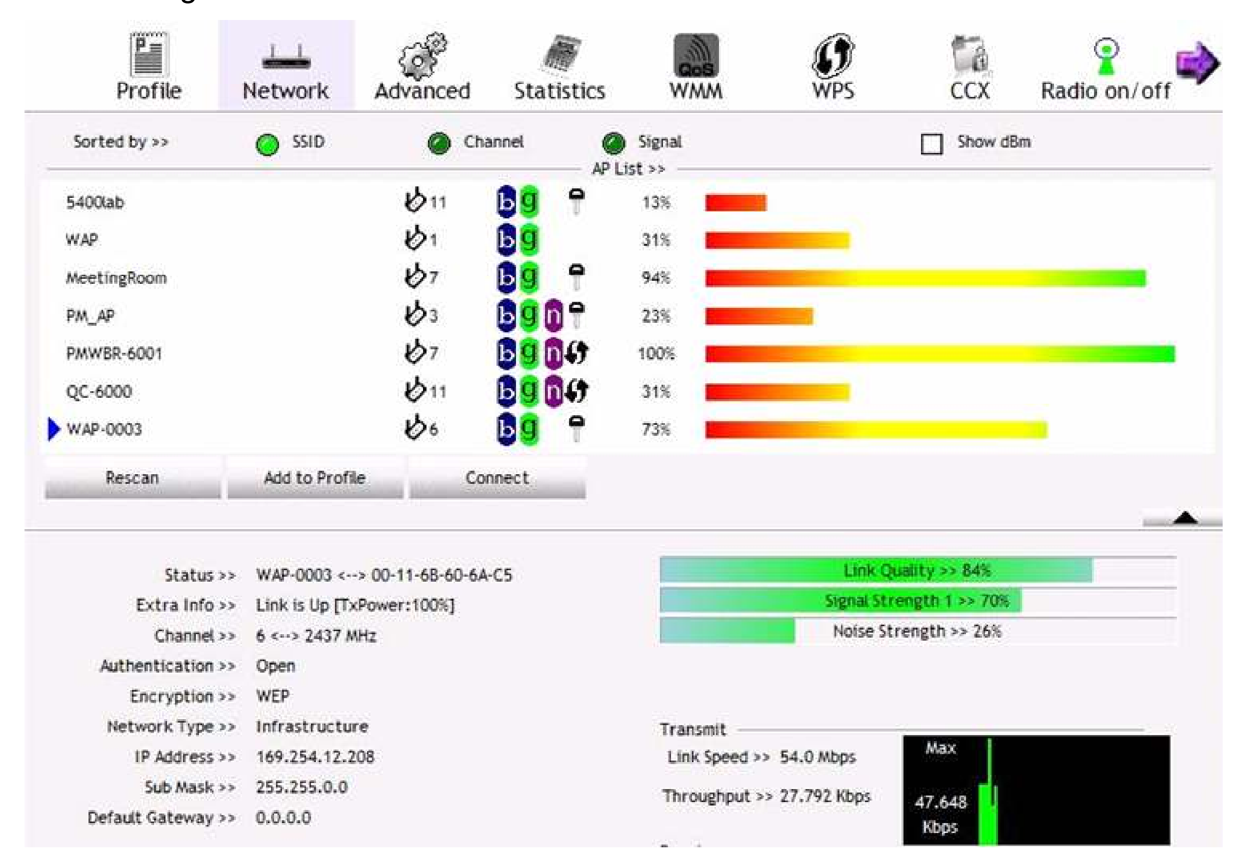
A: Vergewissern Sie sich zuerst, dass das Drahtlos-Clientgerät bereits auf Ihrem Computer installiert ist. Prüfen Sie dann die Konfiguration des Drahtlos-Routers. Die Standardeinstellungen lauten:



Den Drahtlos-Client erkennen Sie am Drahtlossymbol:



Klicken Sie darauf und es blendet sich die Liste mit Zugangspunkten (AP) ein, auf die der Drahtlos-Client zugreifen kann:



Kann der Client Ihren Drahtlos-Router nicht finden, müssen Sie die Netzwerkliste nochmals aktualisieren.

Wählen Sie einen Zugangspunkt (AP) aus und verbinden Sie sich mit ihm:

Bei erfolgreicher Verbindung zeigt Ihr Computer eine Mitteilung ähnlich der Folgenden an.



Sie beziehen jetzt auch das IP vom Router, z.B.:

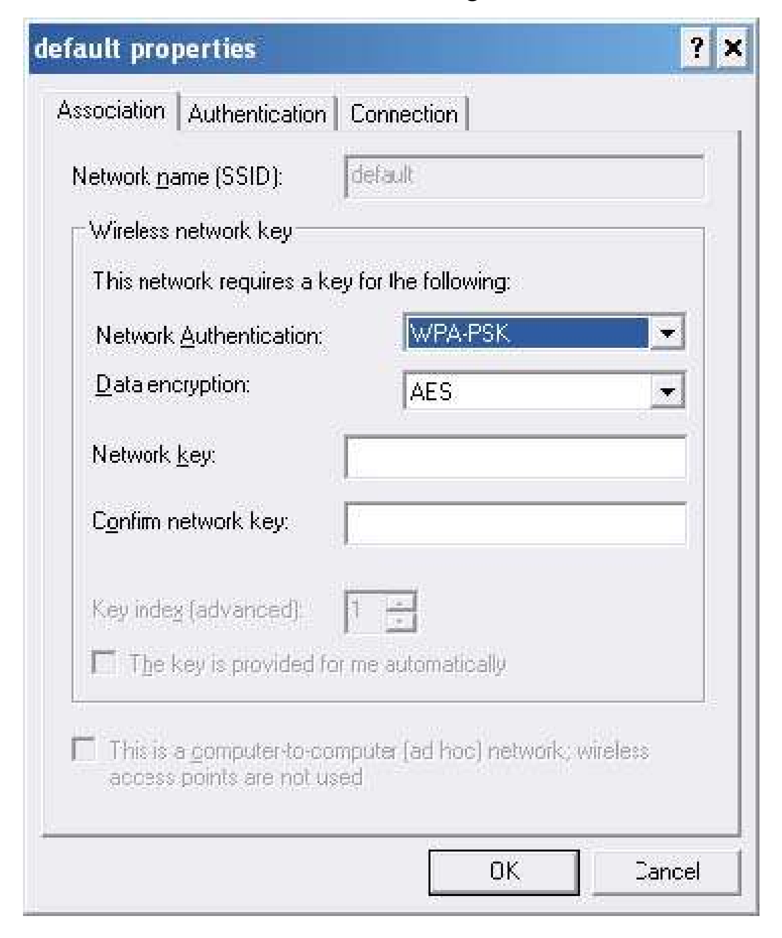
```
Connection-specific DNS Suffix  . :
IP Address. . . . . . . . . . . . : 192.168.0.169
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.0.1
```

2. Wie kann ich mich mit Hilfe der AES-Verschlüsselung von WPA-PSK verbinden?

A: Prüfen Sie zuerst, ob der Treiber vom Drahtlos-Client AES-Verschlüsselung unterstützt. Siehe Folgendes:



Ist SSID auf “default” (Standard) gesetzt, klicken Sie auf “Properties” (Eigenschaften), um zu prüfen, ob der Treiber vom Drahtlos-Client AES-Verschlüsselung unterstützt.



3. Wenn ich den Router drahtlos verbinde, ist das Signal sehr schwach, auch wenn ich ganz in der Nähe des Routers bin.

A: Prüfen Sie zuerst, ob der Drahtlos-Client normal funktioniert. Wenn ja, bringen Sie das Gerät zur Verkaufsstelle, um es dort überprüfen zu lassen.

Technische Daten

Allgemein	
Modell	WBR-6022 *HomeGuard 22 Residential Gateway*
Datenübertragungsrate	1, 2, 5.5, 6, 9, 11, 12, 18, 24, 36, 48, 54 Mbps Max. Rate bis 300 Mbps im 802.11n-Modus
Sendeleistung	802.11b: 17±2 dBm 802.11g: 15±2 dBm 802.11n: 14±2 dBm
Frequenzbereich	Amerika/ FCC: 2,412~2,462 GHz (11 Kanäle) Europa/ ETSI: 2,412~2,472 GHz (13 Kanäle)
Modulationsschemen	DBPSK/DQPSK/CCK/OFDM
Kanäle	1~11 Kanäle (FCC), 1~13 Kanäle (ETSI)
Sicherheit	WEP-Verschlüsselung, WPA-PSK, WPA2-PSK, WPA, WPA2, 802.1x
Diagnose-LED	Ruhezustand Status WAN WLAN LAN
Antenne	2x 2dbi entfernbare und 1x 2dbi interne Antennen
Geräte- und Umgebungsdaten	
Unterstützte Betriebssysteme	Windows 2000, Windows XP, Windows Vista, Linux, MAC OSX
Temperatur	Betrieb: 0° ~ 40°C, Lagerung: -20° ~ 70°C
Luftfeuchte	10% ~ 85% RH, nicht-kondensierend
Abmessungen	187 mm (L) x 112 mm (B) x 29 mm (T)
Zertifizierungen	FCC, CE